

# **Ehdotus sähköisen viestinnän tietosuojalain muuttamiseksi**





Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)		Julkaisun laji	
Sähköisen viestinnän tietosuojalain valmistelutyöryhmä		Työryhmämuistio	
		Toimeksiantaja	
		Liikenne- ja viestintäministeriö	
Puheenjohtaja: ylijohtaja Liisa Ero		Toimielimen asettamispäivämäärä	
Sihteeri: neuvotteleva virkamies Jussi Mäkinen		3.10.2006	
Julkaisun nimi			
Ehdotus sähköisen viestinnän tietosuojalain muuttamiseksi			
Tiivistelmä			
<p>Työryhmän tehtävänä oli laatia ehdotus väärinkäytössäännöksen muuttamiseksi luvattoman käytön ja yrityssalaisuuksien paljastamisen tilanteissa.</p> <p>Työryhmä on kiinnittänyt erityistä huomiota perusoikeuksien tasapainoiseen toteutumiseen. Ehdotetut tunnistamistietojen käsittelyoikeudet eivät koske viestien sisältöjä. Käsittelyoikeudet on pyritty rajamaan siten, että puuttuminen luottamuksellisiin viestintää koskeviin tunnistamistietoihin olisi mahdollisimman vähäistä. Perustuslakivaliokunnan käytännön tai käytettävissä olleiden selvitysten perusteella ei ole saatavissa tarkkaa kuvaa perustuslain sisällöstä ehdotettujen muutosten kannalta.</p> <p>Työryhmä ehdottaa, että yhteisötilaajat saisivat käsitellä tunnistamistietoja maksullisten tietoyhteiskunnan palvelujen luvattoman käytön tai sellaisen viestintäverkon taikka viestintäpalvelun luvattoman käytön havaitsemiseksi, joka on omiaan aiheuttamaan merkittävää haittaa tai vahinkoa yhteisötilaajalle ja yhteisötilaajien oman tai yhteistyökumppanin elinkeinotoiminnan kannalta keskeisten yrityssalaisuuksien paljastamisen selvittämiseksi. Käsittelyoikeus olisi viimesijainen. Yhteisötilaajan tulisi ensisijaisesti pyrkiä suojaamaan viestintäverkkonsa ja palvelunsa sekä yrityssalaisuudet asianmukaisella käyttäjähallinnolla ja asianmukaisin tietoturvatoimin sekä verkon käyttäjille annetuin ohjein.</p> <p>Tunnistamistietojen käsittelyn perusteet ja viestintäverkkojen ja -palvelujen käytöstä annetut ohjeet tulisi ottaa käsiteltäviksi työpaikoilla yhteistoimintamenettelyssä ja niistä tulisi tiedottaa käyttäjille. Käyttäjälle, jonka tietoja on käsitelty, tulisi aina heti ilmoittaa käsittelystä ja sen perusteista. Toimintaa valvoisi tietosuojavaltuutettu.</p> <p>Työryhmä pitää perusteltuna, että ehdotetuista muutoksista hankitaan perustuslakivaliokunnan lausunto, jos asia saatetaan hallituksen esityksellä eduskunnan käsiteltäväksi.</p>			
Avainsanat (asiasanat)			
tunnistamistieto, yhteisötilaaja, yrityssalaisuus, luvaton käyttö			
Muut tiedot			
Yhteyshenkilöt/LVM: Juhapekka Ristola ja Jussi Mäkinen			
Sarjan nimi ja numero		ISSN	ISBN
Liikenne- ja viestintäministeriön julkaisu 29/2007		1457-7488 (painotuote) 1795-4045 (verkkojulkaisu)	978-952-201-886-1 (painotuote) 978-952-201-887-8 (verkkojulkaisu)
Sivumäärä (painotuote)	Kieli	Hinta	Luottamuksellisuus
54	suomi		julkinen
Jakaja		Kustantaja	
Liikenne- ja viestintäministeriö		Liikenne- ja viestintäministeriö	



Författare (uppgifter om organet: organets namn, ordförande, sekreterare)		Typ av publikation	
Arbetsgruppen för beredning av lagen om dataskydd vid elektronisk kommunikation		Arbetsgruppspromemoria	
		Uppdragsgivare	
		Kommunikationsministeriet	
Ordförande, överdirektör Liisa Ero		Datum då organet tillsattes	
Sekreterare, konsultative tjänstemannen Jussi Mäkinen		3.10.2006	
Publikation			
Förslag till ändring av lagen om dataskydd vid elektronisk kommunikation			
Referat			
<p>Arbetsgruppen hade i uppdrag att utarbeta ett förslag för att precisera lagen om dataskydd vid elektronisk kommunikation. Förslaget till ändring gäller bestämmelsen om sammanslutningsabbonenters rätt att behandla identifieringsuppgifter i situationer av olovligt brukande och i fall där företagshemligheter har röjts.</p> <p>Särskild uppmärksamhet har fästs vid att de grundläggande fri- och rättigheterna tillgodoses på ett avvägt sätt. Enligt förslaget skall rätten att behandla konfidentiella identifieringsuppgifter avgränsas så att ingrepp i identifieringsuppgifter som avser elektronisk kommunikation är så små som möjligt. Grundlagsutskottets praxis eller tillbuds stående utredningar ger inte någon exakt bild av förhållandet mellan innehållet i grundlagen och de föreslagna ändringarna.</p> <p>Arbetsgruppen föreslår att sammanslutningsabbonenterna skall få rätt att behandla identifieringsuppgifter för att upptäcka olovligt brukande av avgiftsbelagda informationssamhällstjänster eller olovligt brukande av ett kommunikationsnät eller en kommunikationstjänst, om det olovliga brukandet är ägnat att orsaka betydande men eller skada för sammanslutningsabbonenten. Behandlingen skall vara tillåten också för att utreda fall där företagshemligheter som är väsentliga för sammanslutningsabbonenternas egen eller deras samarbetsparters näringsverksamhet har röjts. Enligt förslaget skall behandlingsrätten tillgripas i sista hand. Sammanslutningsabbonenterna skall i första hand sträva efter att skydda sina kommunikationsnät, tjänster och företagshemligheter med adekvat användaradministration, åtgärder som tryggar informationssäkerheten och med anvisningar till dem som använder kommunikationsnäten. Grunderna för behandlingen av identifieringsuppgifter och anvisningarna för användningen av kommunikationsnät och -tjänster skall enligt förslaget behandlas vid samarbetsförfarandet mellan arbetsgivare och arbetstagare och användarna skall informeras om anvisningarna. Användare vars uppgifter har behandlats manuellt skall alltid omedelbart underrättas om behandlingen. Det föreslås att dataombudsmannen skall ha till uppgift att övervaka verksamheten.</p> <p>Arbetsgruppen anser att det är befogat att begära ett utlåtande om de föreslagna ändringarna av grundlagsutskottet om frågan lämnas till behandling av riksdagen i form av en regeringsproposition.</p>			
Nyckelord			
identifieringsuppgift, sammanslutningsabbonent, företagshemlighet, olovligt brukande			
Övriga uppgifter			
Kontaktpersoner vid ministeriet är Juhapekka Ristola och Jussi Mäkinen.			
Seriens namn och nummer		ISSN	ISBN
Kommunikationsministeriets publikationer 29/2007		1457-7488 (trycksak) 1795-4045 (nätpublikation)	978-952-201-886-1 (trycksak) 978-952-201-887-8 (nätpublikation)
Sidoantal	Språk	Pris	Sekretessgrad
54	finska		offentlig
Distribution		Förlag	
Kommunikationsministeriet		Kommunikationsministeriet	



## DESCRIPTION

Date of publication

1.6.2007

Authors (from body; name, chairman and secretary of the body) Working Group on amending the Act on the Protection of Privacy in Electronic Communications Chair: Liisa Ero, Director-General Secretary: Jussi Mäkinen, Ministerial Adviser	Type of publication Report		
	Assigned by Ministry of Transport and Communications		
	Date when body appointed 3 October 2006		
Name of the publication Amendments to the Act on the Protection of Privacy in Electronic Communications – a working group proposal			
Abstract <p>The working group reviewed the right of corporate and association subscribers to process identification data related to electronic communications. The task of the group was to propose how to amend the Act on the Protection of Privacy in Electronic Communications regarding misuse in cases of unauthorised use of communications services or disclosure of trade secrets.</p> <p>The working group paid special attention to equal exercise of the basic rights. The proposed rights to process identification data do not apply to the content of messages. The aim was to limit the processing rights so that a minimum amount of processing of confidential identification data regarding communications would be needed for solving a particular case. Available studies or the practices by the Constitutional Law Committee do not provide a clear view as to how the proposed amendments relate to Finland's constitution.</p> <p>The working group proposes that corporate or association subscribers would be allowed to process identification data for the purposes of detecting unauthorised use of pay services of the information society or detecting unauthorised use of a communication service or a communications network that is conducive to causing significant damage to the corporate or association subscriber. Corporate and association subscribers are also proposed to be allowed to process identification data in cases of unauthorised disclosure of trade secrets central to their own or their partners' business. However, the right to process the data should be used as a last resort. Corporate and association subscribers should primarily aim to protect their communications networks and services as well as trade secrets with appropriate user administration and information security measures, and by instructing the users about the use of the networks.</p> <p>Guidelines for the processing of identification data and instructions on the use of communications networks and services should be discussed in the cooperation procedure at work places, and the users should be informed of them. Users, whose data have been manually processed, should be informed of the processing immediately.</p> <p>All operations involved in the processing would be supervised by the data protection ombudsman.</p> <p>It is the working group's view that if the matter is submitted to Parliament in the form of a Government proposal, the proposed amendments should be sent to the Constitutional Law Committee for comments.</p>			
Keywords identification data, corporate subscriber, association subscriber, trade secret, unauthorised use			
Miscellaneous Contact persons at the Ministry: Mr Juhapekka Ristola and Mr Jussi Mäkinen			
Serial name and number Publications of the Ministry of Transport and Communications 29/2007		ISSN 1457-7488 (printed version) 1795-4045 (electronic version)	ISBN 978-952-201-886-1 (printed version) 978-952-201-887-8 (electronic version)
Pages, total 54	Language Finnish	Price	Confidence status Public
Distributed and published by Ministry of Transport and Communications			

Liikenne- ja viestintäministeriölle

Liikenne- ja viestintäministeriö asetti 3.10.2006 työryhmän, jonka tehtävänä on laatia ehdotus sähköisen viestinnän tietosuojalain 13 §:n (ns. väärinkäytöspykälä) muuttamiseksi. Ehdotuksessa on tarkasteltava yhteisötilaajan verkko- ja viestintäpalvelujen tunnistamistietojen käsittelyä 1) luvattoman käytön ja 2) yrityssalaisuuksien paljastamisen tilanteissa.

Työryhmän puheenjohtajaksi määrättiin ylijohtaja Liisa Ero liikenne- ja viestintäministeriöstä ja jäseniksi määrättiin viestintäneuvos Juhapekka Ristola liikenne- ja viestintäministeriöstä sekä kutsuttiin lainsäädäntöneuvos Anna-Riitta Wallin oikeusministeriöstä, poliisijohtaja Kimmo Hakonen sisäasiainministeriöstä, hallitusneuvos Raila Kangasperko työministeriöstä, neuvotteleva virkamies Mikael Kiviniemi valtiovarainministeriöstä, lakimies Timo Koskinen Suomen Ammattiliittojen Keskusjärjestö ry:stä, lakimies Pauliina Juntunen Toimihenkilökeskusjärjestö STTK:sta, lakimies Paula Ilveskivi Akava ry:stä ja asiantuntija Mikko Nyssölä Elinkeinoelämän keskusliitosta. Työryhmän sihteerinä on toiminut neuvotteleva virkamies Jussi Mäkinen liikenne- ja viestintäministeriöstä.

Työryhmä on kokoontunut yhteensä kaksitoista kertaa.

Työryhmä on tilannut valtiosääntöoikeudellisen tutkimuksen omaisuuden suojan ja viestinnän luottamuksellisuuden keskinäisestä suhteesta yrityssalaisuuden suojaamisessa sähköisissä verkko- ja viestintäpalveluissa. Työryhmä toteaa, että asiassa esitetyt perusoikeudelliset arvioinnit poikkeavat osin toisistaan. Työryhmässä on kiinnitetty huomiota myös siihen, että ehdotettavaan sääntelyyn liittyy monia oikeudellisesti merkityksellisiä kysymyksiä, kuten seurannan kohteena olevien verkon käyttäjien mahdollisuus huolehtia oikeusturvastaan, sääntelyn tarkkarajaisuus sekä sen suhde muuhun lainsäädäntöön ja muualla laissa omaksuttuihin sääntelytapoihin. Käsiteltävä kokonaisuus on osoittautunut perustuslaillisuuden arvioinnin kannalta, säädösteknisesti ja yhteiskunnalliselta merkitykseltään poikkeuksellisen haastavaksi, minkä vuoksi erityisesti näihin seikkoihin jatkokäsittelyn aikana toivotaan paneuduttavan huolellisesti.

Työryhmä toteaa, että ehdotetut muutokset edellyttävät muutosta myös voimassa olevan lain 13 §:ään. Työryhmä on käsitellyt yksityiskohtaisemmin lakiehdotuksen muotoon laaditun luonnoksen pykälät ja yksityiskohtaiset perustelut. Työryhmä pitää tarpeellisena myös tavanomaisia säädösteknisiä tarkistuksia, joilla ei ole vaikutusta säännösten sisältöön.

Saatuaan työnsä päätökseen työryhmä kunnioittaen luovuttaa liikenne- ja viestintäministeriölle hallituksen esityksen muotoon laaditun luonnoksen.

Helsingissä 1 päivänä kesäkuuta 2007

Liisa Ero

Anna-Riitta Wallin

Kimmo Hakonen

Raila Kangasperko

Mikael Kiviniemi

Timo Koskinen

Pauliina Juntunen

Paula Ilveskivi

Mikko Nyyssölä

Juhapekka Ristola

Jussi Mäkinen

## SISÄLLYS

YHTEENVETO.....	1
SAMMANFATTNING .....	3
SUMMARY .....	5
YLEISPERUSTELUT .....	7
1    Nykytila.....	7
1.1    Lainsäädäntö ja käytäntö .....	7
1.2    Euroopan unionin lainsäädäntö .....	8
1.3    Kansainvälinen kehitys sekä ulkomaiden lainsäädäntö .....	9
1.4    Nykytilan arviointi .....	14
1.5    Keskeiset ehdotukset .....	15
2    Esityksen vaikutukset .....	15
2.1    Taloudelliset vaikutukset.....	15
2.2    Vaikutukset viranomaisten toimintaan .....	16
2.3    Yhteiskunnalliset vaikutukset.....	16
2.4    Tietoyhteiskuntavaikutukset.....	17
2.5    Kansalaisvaikutukset .....	17
3    Asian valmistelu .....	17
3.1    Valmisteluvaiheet ja -aineisto .....	17
3.2    Lausunnot ja jatkovalmistelu.....	17
3.3    Muutosten vaikutusten seuranta .....	18
YKSITYISKOHTAISET PERUSTELUT .....	18
I    Lakiehdotusten perustelut.....	18
II   Voimaantulo .....	28
III  Suhde perustuslakiin ja säätämisyjärjestys.....	28
LAKIEHDOTUKSET .....	34
sähköisen viestinnän tietosuojalain muuttamisesta .....	34
yksityisyyden suojasta työelämässä annetun lain muuttamisesta.....	38
yhteistoiminnasta yrityksissä annetun lain 19 §:n muuttamisesta .....	39
yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 7 §:n muuttamisesta .....	40

## YHTEENVETO

Työryhmä on tarkastellut ehdotuksessaan yhteisötilaajien oikeutta käsitellä sähköisen viestinnän tunnistamistietoja. Sähköisen viestinnän tunnistamistiedot ovat rinnastettavissa kirjeen tai postipaketin osoite- ja postileimatietoihin sekä kirjeen tai paketin kokoon ja muotoon. Käsitteilyoikeus ei koske viestien sisältöjä. Työryhmän tehtävänä oli laatia ehdotus väärinkäytössäänköksen muuttamiseksi luvattoman käytön ja yrityssalaisuuksien paljastamisen tilanteissa. Yhteisötilaajat ovat yksityisiä tai julkisia yhteisöjä, jotka tilaavat viestintäpalvelut käyttäjiensä, esimerkiksi työntekijöidensä käytettäväksi. Yhteisötilaajat hankkivat viestintämahdollisuudet käyttäjilleen pääsääntöisesti elinkeino-, hallinto-, tutkimus- tai muuta toimintaansa varten. Useat yhteisötilaajat sallivat palveluksessaan olevien käyttää viestintäverkkoaan ja viestintäpalveluitaan myös omaan viestintäänsä.

Työryhmä on kiinnittänyt erityistä huomiota perusoikeuksien tasapainoiseen toteutumiseen. Ehdotetut tunnistamistietojen käsittelyoikeudet on pyritty rajaamaan siten, että puuttuminen luottamuksellisiin viestintää koskeviin tunnistamistietoihin olisi mahdollisimman vähäistä tavoiteltuun päämäärään nähden. Perustuslakivaliokunnan käytännön tai käytettävissä olleiden selvitysten perusteella ei ole saatavissa tarkkaa kuvaa perustuslain sisällöstä ehdotettujen muutosten kannalta.

Työryhmä on päätenyt ehdottamaan, että yhteisötilaajat saisivat käsitellä tunnistamistietoja maksullisten tietoyhteiskunnan palvelujen luvattoman käytön tai sellaisen viestintäverkon taikka viestintäpalvelun luvattoman käytön havaitsemiseksi, joka on omiaan aiheuttamaan merkittävää haittaa tai vahinkoa yhteisötilaajalle. Käsittelyoikeus olisi viimesijainen. Yhteisötilaajan tulisi ensisijaisesti pyrkiä suojaamaan viestintäverkkonsa ja palvelunsa asianmukaisella käyttäjähallinnolla ja asianmukaisin tietoturvatoimin. Jos joku tästä huolimatta käyttää verkkoa tai palveluita luvatta, olisi yhteisötilaajalla oikeus käsitellä viestinnän tunnistamistietoja. Tunnistamistietoja saisi käsitellä automaattisen haun avulla, jolloin käyttäjien tunnistamistiedot eivät tulisi kenenkään luonnollisen henkilön tietoon.

Tunnistamistiedot saisi ottaa manuaaliseen käsittelyyn automaattisessa haussa havaitun poikkeaman perusteella tai jos havaittaisiin, että verkossa on esimerkiksi luvatta asennettu laite tai palvelu. Manuaalisesti käsiteltäviksi saisi ottaa ainoastaan asian selvittämisen kannalta välttämättömät tiedot.

Työryhmä ehdottaa, että yhteisötilaajat voisivat käsitellä tunnistamistietoja niiden oman tai yhteistyökumppanin elinkeinotoiminnan kannalta keskeisten yrityssalaisuuksien paljastamisen selvittämiseksi. Käsittely olisi sallittua, jos yrityssalaisuudet on asianmukaisesti suojattu. Yrityssalaisuuksien paljastamisen selvittämiseksi saisi käsitellä vain niiden henkilöiden tietoja, joilla on pääsy yrityssalaisuuksiin. Tunnistamistietoja saisi käsitellä automaattisen haun avulla ja tiedot voisi ottaa manuaalisesti käsiteltäviksi vain automaattisessa haussa havaitun poikkeaman tai yrityssalaisuuden luvattoman julkaisemisen tai muun vastaavan seikan perusteella.

Tunnistamistietojen käsittelyn perusteet ja viestintäverkkojen ja -palvelujen käytöstä annetut ohjeet tulisi ottaa käsiteltäviksi yhteistoimintamenettelyssä ja niistä tulisi tiedottaa käyttäjille.



Käyttäjälle, jonka tietoja on manuaalisesti käsitelty, tulisi aina ilmoittaa käsittelystä ja sen perusteista heti kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Toimintaa valvoisi tietosuojavaltuutettu. Hänelle tulisi ilmoittaa kootusti tiedot vuoden aikana tapahtuneista manuaalisista tunnistamistietojen käsittelytapauksista. Samat tiedot tulisi antaa myös työpaikoilla henkilöstöryhmien edustajille.

Työryhmä pitää perusteltuna, että ehdotetuista muutoksista hankitaan perustuslakivaliokunnan lausunto, jos asia saatetaan hallituksen esityksellä eduskunnan käsiteltäväksi.

## SAMMANFATTNING

En arbetsgrupp tillsatt av kommunikationsministeriet har i sitt förslag sett över sammanslutningsabonnenternas rätt att behandla identifieringsuppgifter vid elektronisk kommunikation. Identifieringsuppgifterna är jämförbara med adress- och stämpeluppgifterna på brev eller postpaket samt med brevetts eller paketets storlek och form. Behandlingsrätten gäller inte innehållet i meddelanden. Arbetsgruppen hade i uppdrag att utarbeta ett förslag för att ändra bestämmelsen om missbruk i händelse av olovligt brukande och om företagshemligheter har röjts. Med sammanslutningsabonnenter avses privata eller offentliga sammanslutningar som abonnerar på kommunikationstjänster som de tillhandahåller exempelvis för sina anställda som är användare av tjänsterna. I regel förser sammanslutningsabonnenterna användarna med de kommunikationsförbindelser som de behöver för den utövade närings-, förvaltnings- eller forskningsverksamheten eller för annan liknande verksamhet. Många sammanslutningsabonnenter tillåter de anställda att använda sitt kommunikationsnät och sina kommunikationstjänster även för privat bruk.

Arbetsgruppen har fäst särskild uppmärksamhet vid att de grundläggande fri- och rättigheterna tillgodoses på ett avvägt sätt. Avsikten har varit att avgränsa den föreslagna rätten att behandla konfidentiella identifieringsuppgifter så att ingrepp i identifieringsuppgifter som avser kommunikation skall vara så små som möjligt med tanke på det eftersträlvade syftet med behandlingen. Grundlagsutskottets praxis eller tillbuds stående utredningar ger inte någon exakt bild av förhållandet mellan innehållet i grundlagen och de föreslagna ändringarna.

Arbetsgruppen föreslår att sammanslutningsabonnenterna skall få rätt att behandla identifieringsuppgifter för att upptäcka olovligt bruk av avgiftsbelagda informationssamhällstjänster eller olovligt brukande av ett kommunikationsnät eller en kommunikationstjänst, om det olovliga brukandet är ägnat att orsaka betydande men eller skada för sammanslutningsabonnenten. Enligt förslaget skall behandlingsrätten tillgripas i sista hand. Sammanslutningsabonnenterna skall i första hand sträva efter att skydda sitt kommunikationsnät och sina tjänster med adekvat användaradministration och lämpliga åtgärder som tryggar informationssäkerheten. Om någon trots detta olovligen brukar nätet eller tjänsterna i det föreslås sammanslutningsabonnenten ha rätt att behandla de identifieringsuppgifter som uppkommer vid elektronisk kommunikation. Det föreslås att identifieringsuppgifterna skall behandlas med hjälp av en automatisk sökning så att ingen fysisk person får kännedom om användarnas identifieringsuppgifter.

Enligt förslaget skall det vara tillåtet att ta identifieringsuppgifterna till manuell behandling på basis av en avvikelse som den automatiska sökningen har uppdagat eller om det kommer fram att t.ex. en anordning eller tjänst obehörigen har installerats i nätet. En manuell behandling av uppgifterna skall vara tillåten endast om detta är nödvändigt för att reda ut avvikelsen.

Arbetsgruppen föreslår att sammanslutningsabonnenter skall få behandla identifieringsuppgifter för att utreda fall där företagshemligheter som är väsentliga för deras egen eller deras samarbetspartners näringsverksamhet har röjts. Behandlingen avses vara tillåten om företagshemligheterna har skyddats på tillbörligt sätt. För att utreda röjande av företagshemligheter skall det enligt förslaget vara tillåtet att behandla endast sådana personers uppgifter, som har till-

gång till företagshemligheter. Det avses vara tillåtet att behandla identifieringsuppgifter med hjälp av en automatisk sökning och att ta uppgifterna till manuell behandling endast till följd av en avvikelse som har uppdagats vid den automatiska sökningen, olovligt offentliggörande av företagshemlighet eller någon annan motsvarande omständighet.

Grunderna för behandlingen av identifieringsuppgifter och anvisningarna för användningen av kommunikationsnät och kommunikationstjänster skall behandlas vid samarbetsförfaranden mellan ledningen och personalen och användarna skall informeras om dem. Användare vars uppgifter har behandlats manuellt skall enligt förslaget alltid underrättas om behandlingen och grunderna för den genast då detta kan ske utan att äventyra behandlingens syfte. Det föreslås att verksamheten skall övervakas av dataombudsmannen. Dataombudsmannen skall enligt förslaget på ett samlat sätt underrättas om alla de gånger under ett år då identifieringsuppgifter har behandlats manuellt. Samma uppgifter bör även lämnas till personalgruppernas representanter på arbetsplatserna.

Arbetsgruppen anser det vara befogat att ett utlåtande om de föreslagna ändringarna begärs av grundlagsutskottet i fall att frågan lämnas till behandling av riksdagen i form av en regeringsproposition.

## SUMMARY

The working group reviewed the right of corporate and association subscribers to process identification data related to electronic communications. Identification data in electronic communications can be compared to the address and postmark information or the size and form of a letter or a postal package. The right of corporate and association subscribers to process identification data does not apply to the content of messages. The task of the working group was to draw up a proposal on amending the provisions of law regarding misuse in cases of unauthorised use or disclosure of trade secrets. Corporate or association subscribers are private or public corporations or organisations that subscribe communications services for the use of, for example, their employees. The corporate and association subscribers mainly acquire access to means of communication to their users for such purposes as business, administrative, research and development activities. Several corporate or association subscribers allow their employees to use the corporate or association communications network and services for the employees' personal communications too.

The working group paid special attention to equal exercise of the basic rights. The aim of the group was to limit the rights to process identification data so that a minimum amount of processing of confidential identification data regarding communications would be needed for reaching the desired result. Available studies or the practices by the Constitutional Law Committee do not provide a clear view as to how the proposed amendments relate to Finland's constitution.

The working group proposes that corporate or association subscribers would be allowed to process identification data to detect unauthorised use of pay services provided by the information society or to detect unauthorised use of a communication service or a communications network that is conducive to causing significant damage to the corporate or association subscriber. The right to process the data should be used as a last resort. Corporate and association subscribers should primarily aim to protect their communications networks and services with appropriate user administration and information security measures. If anyone, despite of this, uses the network or services without due authorisation, the corporate or association subscriber would have the right to process the identification data related to communications. The identification data could be processed by means of an automatic search function, which would not let any natural person to have access to the users' identification data.

It would be permitted to process the identification data manually, if a deviation was detected in the automatic search or a device or service was installed in the network without permission. Manual processing would be allowed only of the data necessary for resolving the matter at hand.

The working group proposes that corporate and association subscribers be allowed to process identification data in cases of unauthorised disclosure of trade secrets central to their own or their partners' business. The processing would be allowed if the trade secrets were appropriately protected. In order to examine disclosures of trade secrets only the data involving persons who have access to trade secrets would be open for processing. The identification data

could be processed by means of an automatic search and the data taken up for manual processing only if a deviation was detected in the automatic search or a trade secret was disclosed and published without a due authorisation or because of some other similar reason.

The guidelines for the processing of identification data and the instructions on the use of communications networks and services should be discussed in the cooperation procedure at work places, and the users should be informed of them. Users, whose data have been manually processed, should always be informed of the processing and its basis as soon as it is possible without endangering the purpose of the processing itself. The operations involved would be supervised by the data protection ombudsman. He or she should be given an annual compilation of data on manual processing transactions. The same information should also be given to the representatives of employee groups.

It is the working group's view that if the matter is submitted to Parliament in the form of a Government proposal, the proposed amendments should be sent to the Constitutional Law Committee for comments.

## 1 Nykytila

### 1.1 Lainsäädäntö ja käytäntö

Sähköisen viestinnän tietosuojalaissa (516/2004) on säädetty sähköisten viestien välittäjien velvollisuuksista, joilla taataan viestinnän luottamuksellisuus ja viestintäverkkojen käyttäjien yksityisyys tavallisen lain tasolla. Perustuslain tasolla yksityiselämän eli yksityisyyden suojasta säädetään perustuslain 10 §:ssä. Yksityisyyden suojaan kuuluu myös viestinnän luottamuksellisuus, mikä tarkoittaa sitä, että viestin sisällön suojan lisäksi suoja ulottuu myös niihin tunnistamistietoihin, joista voidaan tunnistaa luonnollinen henkilö. Sähköisen viestinnän tietosuojalaissa viestinnän luottamuksellisuuden takaava sääntely ulotettiin koskemaan teleyrityksien lisäksi myös yhteisötilaajia. Yhteisötilaajia ovat viestintäpalvelun tai lisäarvopalvelun tilaajana olevat yritykset tai yhteisöt, jotka käsittelevät viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja.

Sähköisen viestinnän tietosuojalain 4 §:n 1 momentin mukaan viesti, tunnistamistiedot ja paikkatiedot ovat luottamuksellisia, jollei sähköisen viestinnän tietosuojalaissa tai muussa laissa toisin säädetä. Sähköisen viestinnän tietosuojalain 9–14 §:ssä on säädetty niistä tilanteista, joissa joku muu kuin viestinnän osapuoli voi käsitellä tunnistamistietoja.

Lain 2 §:n määritelmän mukaan tunnistamistiedoilla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Tunnistamistietoihin voi kuulua tietoja, jotka viittaavat muun muassa viestinnän reititykseen, keston, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan, lähettäjän tai vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähettävään tai vastaanottavaan verkkoon ja yhteyden alkuun, loppuun tai

keston. Tiedot voivat myös koskea muotoa, jossa viesti välitetään verkossa.

Perinteiseen postitoimintaan verrattaessa sähköisen viestinnän tunnistamistiedot ovat rinnastettavissa kirjeen tai postipaketin osoite- ja postileimatietoihin sekä kirjeen tai paketin kokoon ja muotoon.

Lain 9 §:n mukaan tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä näiden tietoturvasta huolehtimiseksi. Lisäksi tunnistamistietoja saa käsitellä laskutusta, markkinointia, teknistä kehittämistä ja palvelun käyttöä koskevien väärinkäytösten sekä vika- ja häiriötilanteiden havaitsemiseksi.

Lain 8 §:n 3 momentin mukaan tunnistamistietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa, eikä sillä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tunnistamistietoja on sallittua luovuttaa ainoastaan niille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä.

Sellaiset tunnistamistiedot, joista on tunnistettavissa luonnollinen henkilö, ovat myös henkilötietoja. Lain 3 §:n soveltamisalasäännöksen mukaan henkilötietojen käsittelyyn sovelletaan, mitä henkilötietolaissa (523/1999) säädetään, jollei tästä laista muuta johdu.

Viestintäverkkojen väärinkäytösten ja yrityssalaisuuksien oikeudettoman paljastamisen selvittämisessä ovat käytettävissä tietohallinnolliset keinot, kuten käyttäjätietolokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näiden tietojen käsittelylle ei sähköisen viestinnän tietosuojalaissa aseteta rajoituksia. Toisaalta näiden tietojen avulla pystytään vain poik-

keuksellisesti selvittämään väärinkäytökset kokonaisuudessaan.

Toisin sanoen tietojärjestelmiä voidaan seurata vapaasti muun muassa väärinkäytöksiä selvitetessä erilaisten käyttäjä-, tallennus- ja muiden sellaisten lokitietojen avulla.

Yksityisyyden suojasta työelämässä annetun lain (759/2004) 6 luvussa on säädetty työnantajalle kuuluvien sähköpostien esille hakemisesta ja avaamisesta sekä tähän liittyvästä menettelystä työntekijän ollessa estynyt hoitamaan työtehtäviään. Lain 18 §:n mukaan työnantajalla on oikeus hakea esille ja avata työntekijän käyttöön osoittaman sähköpostin viestejä vain, jos työnantaja on toteuttanut sanottujen viestien suojaksi laissa määritellyt tarpeelliset toimenpiteet.

Yksityisyyden suojasta työelämässä annetun lain 19 §:ssä on tarkemmin säädetty niistä perusteista, jolloin työnantaja voi hakea esille otsikkotietojen avulla työntekijän sähköpostiosoitteeseen saapuneet tai siitä lähetetyt viestit, joista työnantajan on välttämätöntä saada tieto toimintaansa liittyvien neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai muutoin toimintojensa turvaamiseksi.

Yksityisyyden suojasta työelämässä annetun lain 20 §:n mukaan työnantaja saa myös avata hänelle kuuluvat viestit, jos on ilmeistä, että viestin otsikkotiedon perusteella viesti on tarkoitettu työnantajalle ja tiedon saaminen siitä on välttämätöntä, eikä viestin lähettäjään tai vastaanottajaan saada yhteyttä viestin sisällön selvittämiseksi eikä viestiä voida toimittaa toiseen osoitteeseen.

Viestin esille hakemisesta ja avaamisesta on laadittava siihen osallistuneiden henkilöiden allekirjoittama selvitys, josta ilmenee mikä viesti on avattu, miksi viesti on avattu, avaamisen ajankohta, avaamisen suorittajat sekä kenelle avatun viestin sisällöstä on annettu tieto. Selvitys on ilman aiheutonta viivytystä toimitettava työntekijälle.

Viestinnän luottamuksellisuuden loukkaukset on kriminalisoitu rikoslain (39/1889) 38 luvun 3 ja 4 §:ssä säädetään viestintäsalaisuuden loukkaus rangaistavaksi teoksi. Rikoslain 38 luvun 3 §:ssä säädetään rangaistus sille, joka oikeudettomasti avaa toiselle osoitetun kirjeen tai

muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä tai hankkii tiedon televerkossa välitetävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta.

Liikesalaisuuksien suojasta on säädetty sopimattomasta menettelystä elinkeinotoiminnassa annetun lain (1061/1978) 4 §:ssä. Rikoslain 30 luvun 4–6 §:ssä on kriminalisoitu yritysvakoilu, yrityssalaisuuden rikkominen ja yrityssalaisuuden väärinkäyttö. Rikoslaisissa omaksuttu yrityssalaisuuden käsite kattaa sekä liike- että ammattisalaisuudet. Liike- ja ammattisalaisuuksien suojasta on lisäksi säädöksiä useissa muissa laeissa.

Pakkokeinolain (450/1987) 5 a luvun 3 §:n mukaan televalvonta on mahdollista muun muassa sellaisten rikosten tutkinnassa, joista ankarin rangaistus on 4 vuotta vankeutta tai jotka kohdistuvat automaattiseen tietojenkäsittelyjärjestelmään. Koska yrityssalaisuusrikoksien enimmäisrangaistukset ovat kaksi vuotta vankeutta, televalvontaa voidaan käyttää vain sellaisen yritysvakoilun tutkinnassa joka samalla täytäisi rikoslain 38 luvun 8 §:ssä tarkoitetun tietomurron tunnusmerkit.

Yksityisyyden suojasta työelämässä annetun lain perusteella työnantaja voidaan tuomita sakkorangaistukseen, jos muualla laissa ei ole säädetty ankarampaa rangaistusta.

Voimassa oleva sähköisen viestinnän tietosuojalaki ei salli tunnistamistietojen käsittelyä yrityssalaisuuksien oikeudettoman paljastamisen selvittämiseksi.

## 1.2 Euroopan unionin lainsäädäntö

Euroopan parlamentin ja neuvoston 24 päivänä lokakuuta 1995 antama direktiivi 95/46/EY yksilöiden suojelusta ja henkilötietojen käsittelystä ja näiden tietojen vapaasta liikkuvuudesta, myöhemmin *henkilötietodirektiivi* on pantu täytäntöön henkilötietolailla (523/1999). Direktiivillä on pyritty turvaamaan yksilöiden perusoikeudet ja yksityisyys henkilötietoja käsiteltäessä.

Euroopan parlamentin ja neuvoston 12 päivänä heinäkuuta 2002 antama direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, myöhemmin *sähköisen viestinnän tietosuojadirektiivi*, pantiin kansallisesti täytäntöön sähköisen viestinnän tietosuojalailla, joka tuli voimaan syyskuussa 2004.

Direktiivin 5 artiklassa on säädetty jäsenvaltioiden velvollisuudesta varmistaa yleisessä viestintäverkossa ja sähköisten viestintäpalveluiden välityksellä tapahtuvan viestinnän luottamuksellisuus.

Direktiivin 15 artiklassa on säädetty jäsenvaltioiden mahdollisuudesta toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan muun muassa direktiivin 5 artiklan mukaisten oikeuksien ja velvollisuuksien soveltamisalaa. Rajoitusten on oltava välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden (valtion turvallisuus) sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi henkilötietodirektiivin 13 artiklan 1 kohdan mukaisesti.

### 1.3 Kansainvälinen kehitys sekä ulkomaiden lainsäädäntö

Voimassa oleva sääntely perustuu keskeisiltä osin sähköisen viestinnän tietosuojadirektiiviin. Direktiivin kansallisesa täytäntöönpanossa viestinnän luottamuksellisuuden takaavat velvoitteet ulotettiin koskemaan myös yhteisötilaajia.

Tässä ehdotuksessa esitetyt sääntelyn muutokset ovat pääosin kansallisen täytäntöönpanon yksityiskohtiin ja voimassa olevan kansallisen sääntelyn soveltamisessa ja tulkinnassa esiin tulleiden ongelmien korjaamiseen liittyviä ehdotuksia. Sähköisen viestinnän tietosuojalain yhteisötilaajan käsitettä ei ole omaksuttu muissa maissa. Tämän vuoksi kansainvälisessä vertailussa on keskitytty yleisesti yksityiselämän suojaa, yrityssalaisuuksien suojaa, henkilötietojen suojaa ja sähköisen viestinnän tietosuojaa koskevan lainsäädännön esittelyyn.

### Ruotsi

Ruotsin perustuslaki koostuu neljästä säädöksestä. Näitä säädöksiä ovat hallitusmuoto (Regeringsform SFS 1974:152), perimysjärjestys, painovapausasetus (Tryckfrihetsförordning SFS 1949:105) ja sananvapauden perustuslaki (Yttrandefrihetsgrundlag SFS 991:1469). Nämä lait toimivat Ruotsissa poliittisen päätöksenteon pohjana ja sisältävät useita yksityisyyden suojan, kansalaisvapauksien ja ihmisoikeuksien kannalta merkityksellisiä säännöksiä. Hallitusmuodon 2 § sisältää säännöksen yksityisyyden suojasta. Hallitusmuodon 2 luvun 13 §:ssä todetaan, että ilmaisun ja tiedon liikkumisen vapautta, joita sananvapausasetus perustuslaillisesti suojaa, voidaan rajoittaa yksityiselämän koskemattomuuden suojaamiseksi. Hallitusmuodon 2 luvun 3 § turvaa lisäksi yksityiselämän koskemattomuuden, kun kyse on automaattisesta tietojenkäsittelystä.

Ruotsissa on säädetty erityinen laki yrityssalaisuuksien suojasta (Lag om skydd för företagshemligheter 1990:40). Lain 1§:n mukaan yrityssalaisuudella tarkoitetaan sellaista tietoa, jota elinkeinonharjoittaja liike- tai muussa toiminnassa pitää salaisena ja jonka paljastuminen on omiaan aiheuttamaan hänen liiketoiminnalleen vahinkoa heikentämällä kilpailun edellytyksiä. Tiedolla tarkoitetaan sekä eri tavoin dokumentoitua tietoa, mukaan lukien piirrookset, mallit ja vastaavat tekniset kuvaukset, että yksittäisten henkilöiden hallussaan pitämää tietoa jostain seikasta, vaikka sitä ei olisikaan dokumentoitu. Työntekijän, joka tahallaan tai huolimattomuudella käyttää hyväkseen tai paljastaa työnantajan yrityssalaisuuden, jonka on saanut tietoonsa työsuhteessa olosuhteissa, joissa hän käsittelee tai hänen olisi pitänyt käsitellä, ettei tietoa saa paljastaa, on korvattava toiminnastaan aiheutunut vahinko (7 §). Jos teko on tapahtunut työsuhteen päättyttyä, sovelletaan säännöstä vain, jos siihen on erityisiä syitä. Tällaiset tilanteet korostavat salassapitosopimusten merkitystä.

Ruotsin keskeinen tietosuojalaki on henkilötietolaki (Personuppgiftslag, 1998:204), jolla on pantu täytäntöön EU:n henkilötietodirektiivi. Laki sääntelee automatisoitujen henkilörekisterien käyttöä sekä julkisella että yksityisellä sektorilla.



Ruotsissa ei ole erillistä lakia koskien työelämän yksityisyyden suojaa, vaan näitä kysymyksiä säännellään henkilötietolaissa. Erillinen työelämän tietosuojaa koskeva lainvalmistelu on vireillä ja lakiehdotus annettaneen vuoden 2008 alkupuolella.

Työntekijöiden henkilötietoja voidaan käsitellä vain lain sallimissa tilanteissa. Henkilötietojen käsittelyn tarkoitus on määriteltävä, eikä tietoja saa käsitellä muita tarkoituksia varten. Tarkoituksesta on informoitava niitä, joiden tietoja käsitellään. Lain sallimia tilanteita, joissa henkilötietoja voidaan käsitellä, ovat suostumukseen perustuva käsittely, sopimukseen perustuva käsittely, jolloin työntekijä ja työnantaja ovat sopineet henkilötietojen käsittelystä sopimuksen toteuttamiseksi sekä käsittely oikeudellisen velvoitteen täyttämiseksi. Samoin henkilötietoja voi käsitellä työntekijän tärkeän edun suojaamiseksi tai jos tietoja käytetään työtehtävän suorittamiseen viranomaisessa sekä muissa tapauksissa, joissa työnantajan tai muun henkilön, jolle henkilötiedot luovutetaan, intressi on suurempi kuin työntekijän yksityisyyden. Työnantajan oikeus valvontaan työpaikoilla on ratkaistu Ruotsin oikeuskäytännössä intressipunninnalla, jossa vertaillaan työnantajan direktio-oikeutta ja työntekijöiden yksityisyyden suojaa. Yksityisyyttä rajoittavien toimenpiteiden pitää olla oikeassa suhteessa tavoiteltuun päämäärään nähden.

Sähköisen viestinnän tietosuojadirektiivi on pantu Ruotsissa täytäntöön lailla sähköisestä viestinnästä (Lag om elektronisk kommunikation, 2000:389). Sähköisen viestinnän laki sääntelee myös viestintämarkkinakysymyksiä, sillä lailla on pantu täytäntöön koko EU:n viiden tietoliikennettä koskevan direktiivin lainsäädäntöpaketti. Ruotsissa ei siten ole erillistä sähköisen viestinnän tietosuojalakia. Ruotsin sähköisen viestinnän lain sääntely kohdistuu ainoastaan teleyrityksiin ja lisäarvo palvelun tarjoajiin eikä yhteisötilaajiin, jotka käsittelevät viestintäverkossaan käyttäjien luottamuksellisia viestejä tunnistamistietoja tai paikkatietoja.

Sähköisen viestinnän lain 2 §:n mukaan henkilötietolaki soveltuu myös tietoverkkojen ja sähköisten viestintäpalvelujen käyttöön, ellei laista muuta johdu.

## Norja

Norjan perustuslaki on vuodelta 1814 (Kongerikets Norges Grundlov). Perustuslaki on muodoltaan hieman muista kansainvälisen vertailun kohdemaista poikkeava, sillä se ei sisällä nimenomaista yksityiselämän suojaa koskevaa määräystä. Yksityisyyden suoja on kehittynyt Norjassa oikeuskäytännön myötä. Vuonna 1952 Norjan korkein oikeus totesi, että henkilöllisyys nauttii Norjan oikeudessa suojaa ja henkilöllisyyden suoja käsittää yksityiselämän suojan. Norja ei ole Euroopan unionin jäsen, mutta on osa Euroopan talousaluetta, joten niin sanottu ensimmäisen pilarin lainsäädäntö, johon tietosuojaa ja sähköistä kaupankäyntiä koskevat direktiivit kuuluvat, on Norjaa sitovaa.

Norjassa ei ole erillistä lakia yritysalaisuuksien suojasta, vaan asiasta on säädetty vuonna 1972 säädetyssä markkina-laissa (Lov om kontroll med markedsföring og avtalevilkår, markedsføringsloven).

Norjan nykyinen tietosuojalaki (Lov om behandling av personopplysninger), on vuodelta 2000. Sitä täydentää tietosuojasetus (Forskrift om behandling av personopplysninger). Laki perustuu henkilötietodirektiiviin, joten sen määräykset ovat lähes kauttaaltaan samansisältöiset kuin direktiivin.

Norjassa sähköisen viestinnän tietosuojadirektiivi on pantu täytäntöön sähköistä viestintää koskevalla yleislailla eli Ekomlovenilla (Lov om elektronisk kommunikasjon).

Norjassa ei ole erillistä lakia yksityisyyden suojasta työelämässä, vaan asiaa on ohjeistettu Datatilsynetin ohjeilla. Pääsääntönä on, että työnantajan halutessa lukea työntekijän sähköpostia ja muita tietokansioita, tämä tarvitsee työntekijän suostumuksen tai asia ratkaistaan Norjan tietosuojalain 8 § f -kohdan ja direktiivin tarkoittaman intressivertailun perusteella. Norjalainen työnantaja voi päättää direktio-oikeutensa perusteella, että työhön liittyviin tarkoituksiin on käytettävä työnantajan tietojärjestelmiä. Työnantajan on laadittava säännöt tietojärjestelmän käytölle, jolloin on täsmennettävä, missä laajuudessa järjestelmää voidaan käyttää yksityisiin tarkoituksiin. Näissä säännöissä, jotka on liitettävä yrityksen sisäisen tarkastuksen

sääntöihin, on ilmaistava, missä olosuhteissa työnantaja voi lukea yksityistä sähköpostia. Lähtökohtana on, että jos tällaisia sääntöjä ei ole, ei työnantaja ole oikeutettu lukemaan työntekijän sähköpostia.

Mikäli työnantaja epäilee työntekijää epälojaaliudesta tai tämän toimivan sisäisten sääntöjen ja ohjeiden vastaisesti, voi työnantajalle syntyä oikeus tarkastaa työntekijän sähköposti- ja kirjeenvaihtoa. Jos työnantajalla on riittävät perustelut epäilyksille, voi asiallisten perustelujen vaatimus tarkastuksille täyttyä. Mikäli työnantajan tarkastusintressit konkreettisesti tapauksessa ovat suurempia kuin työntekijän oikeus yksityisyyteen, voidaan tarkastus suorittaa ilman työntekijän suostumusta.

### *Tanska*

Tanskan vuodelta 1953 peräisin oleva perustuslaki sisältää kaksi yksityisyyden suojaa koskevaa määräystä. Perustuslain 71 § takaa kansalaisen henkilökohtaisen koskemattomuuden. Tanskan kansalaisen vapautta ei voi riistää poliittisen tai uskonnollisen vakaumuksen vuoksi tai syntyperän johdosta.

Perustuslain 72 § määrää kotirauhan loukkaamattomaksi. Kotietsintä, kirjeiden ja muun kirjallisen aineiston takavarikointi ja tutkiminen, samoin kuin postin, tietoliikenne- ja puhelinsalaisuuden murtaminen voi tapahtua ainoastaan oikeuden määräyksellä, ellei laissa ole toisin määrätty. Lainkohta soveltuu kaikkeen tietoliikenteeseen ja sähköiseen tietoon.

Tanskan markkinointilaki (Maerkedsfoeringsloven 1389, 21.12.2005) sääntelee yrityssalaisuuksien suojaa. Lain 19 §:n mukaan henkilö, joka on palvelussuhteessa yritykseen tai toimii yhteistyössä sen kanssa tai joka suorittaa tehtävää yrityksen lukuun ei saa hankkia tai yrittää hankkia tietoonsa tai haltuunsa kyseisen yrityksen yrityssalaisuuksia luvottomasti. Jos edellä mainittu henkilö on hankkinut tiedon yrityssalaisuudesta laillisesti, hän ei saa ilman asianmukaista lupaa luovuttaa tai käyttää yrityssalaisuutta. Kielto on voimassa kolme vuotta palvelusuhteen, yhteistyön tai tehtävän päättymisestä. Näitä sääntöjä sovelletaan samalla tavoin muuhun henkilöön, jolla on laillinen pääsy yritystietoon.

Tanskan tietosuojalaki (Lov om behandling af personoplysninger nr 429, 31.5.2000) on vuodelta 2000. Lailla on pantu täytäntöön henkilötietodirektiivi. Sähköisen viestinnän tietosuojamääräykset sisältyvät telelainsäädännön vuoden 2003 muutokseen (Lov om konkurrence- og forbrugerforhold på telemarkedet Lov nr. 418 af 31. maj 2000), jolla sähköisen viestinnän tietosuojadirektiivi pantiin täytäntöön.

Tanskassa ei ole erillistä työelämän tietosuojalakia, vaan työelämän yksityisyyden suojaa säännellään henkilötietolain pohjalta. Maan viranomaiset eivät ole ottaneet erityisen jyrkkää kantaa yksityisyyden suojaamiseen työelämässä. Tanskan tietosuojalaki tarjoaa työnantajalle mahdollisuuden kerätä ja jopa paljastaa henkilötietoja ilman työntekijän suostumusta, milloin tämä on välttämätöntä oikeudellisen veloitteen täyttämiseksi, yhteiskunnan kannalta merkityksellinen tehtävän suorittamiseksi tai laillisen tarpeen täyttämiseksi, joka menee työntekijän edun edelle.

### *Saksa*

Saksan liittotasavallan perustuslaki (*Grundgesetz*) on vuodelta 1949, ja sitä on viimeksi muutettu Saksojen jälleenyhdistymisen yhteydessä 1990. Perustuslain 10 artiklassa turvataan kirje- ja tietoliikennesalaisuus ja poikkeuksia tähän voidaan tehdä ainoastaan lain säännösin. Silloin, kun rajoituksen tarkoituksena on demokraattisen yhteiskuntajärjestelmän tai liittovaltion turvallisuuden turvaaminen, voidaan lainsäädännössä määrätä, ettei kajoamisen kohteeksi joutunut henkilö saa tietää toimenpiteestä. Tuomioistuimien asemesta oikeusturvatiensä toimivat tällöin liittopäivien nimeämät elimet.

Perustuslain turvaamasta viestintäsalaisuudesta säädetään tarkemmin telekommunikaatiolain eli Telekommunikationsgesetzin 85 §:ssä. Viestintäsalaisuus ulottuu myös yhteydenottoyrityksiin. Telekommunikaatiolain 86 §:ssä säädetään telekuuntelun kiellosta sekä vastaanottolaitteiden ylläpitäjän salassapitovelvollisuudesta. Vastaavasti lain 87 §:ssä säädetään ammattimaisessa tarkoituksessa tietoliikennelaitteita ylläpitävän henkilön velvollisuudesta ylläpitää teknisiä suojakeinoja

muun muassa viestintäsalaisuuden ylläpitämiseksi.

Pakkokeinoista, myös tietoliikennettä koskevista, säädetään rikosprosessijärjestyksessä eli Strafprozessordnungissa (StPO).

Saksassa yrityssalaisuuksien suojasta säädetään vilpillistä kilpailua koskevan lain 17 §:ssä. Yrityssalaisuuden piiriin kuuluu kaupallisesti arvokas tieto, joka ei ole julkisesti saatavilla ja se, jolle tieto kuuluu, on ilmaissut objektiivisen aikomuksen tiedon salassa pitämiseksi. Lainkohdan 1 momentin mukaan rangaistaan sellaista työntekijää, oppisopimuskoulutuksessa olevaa tai muuta henkilöä, joka työsuhteen kuluessa ilmaisee ilman lupaa kolmannelle kauppa- tai teollisuussalaisuuden, joka on hänelle uskottu tai saatettu hänen tietoonsa työsuhteen puitteissa, jos hän tekee paljastuksen kilpailun tai henkilökohtaisen edun vuoksi, hyödyttääkseen kolmatta osapuolta tai vahingoittaakseen elinkeinonharjoittajaa. Vilpillistä kilpailua koskevan lain 17 §:n 2 momentin mukaan rangaistaan henkilöä, jotka yllä kuvatuista syistä hankkii luvatta kauppa- tai teollisuussalaisuuden käyttämällä teknisiä keinoja, luomalla salaisuuden sisältävän kopion tai irrottamalla esineen, johon salaisuus on sisällytetty. Sama koskee henkilöä, joka käyttää tai ilmaisee toiselle kaupallisen tai teollisen salaisuuden, jonka on hankkinut tai saanut ilman lupaa sen luvatta ilmaiselta työntekijältä tai oman tai toisen henkilön toiminnan tuloksena.

Saksassa on Euroopan Unionin tiukimpia tietosuojalakeja. Maailman ensimmäinen tietosuojalaki säädettiin vuonna 1970 Hessenin osavaltiossa. Saksan nykyinen tietosuojalaki (Bundesdatenschutzgesetz) on vuodelta 1990, ja se on viimeksi uudistettu vuonna 2002. Laki antaa rekisteröidyille laajat mahdollisuudet vastustaa tiedon käsittelyä. Laki vaatii yrityksen nimeävän tietosuojavastaavan, jos yritys kerää, käsittelee tai käyttää henkilötietoja. Henkilötietoja sisältävät tietokannat on rekisteröitävä tietosuojaviranomaisessa. Rekisteröitävän antaman suostumuksen merkitystä on korostettu.

Sähköisen viestinnän tietosuojaa koskevat määräykset sisältyvät vuonna 2004 muutettuun telekommunikaatiolakiin, jo-

hon yhdistettiin vuoden 2000 tietoliikennettä koskeva tietosuoja-asetus.

### *Viro*

Viron nykyinen perustuslaki on vuodelta 1992. Laki tunnustaa oikeuden yksityisyyteen, viestinnän luottamuksellisuuteen sekä, ainakin osittain, tietosuojaan. Perustuslain artikla 42 toteaa, ettei valtion tai paikallisen hallinnon viranomainen voi kerätä tietoa Viron kansalaisen vakaumuksesta vastoin tämän tahtoa.

Artikla 43 lisää, että jokaisella on oikeus luottamukselliseen viestintään kirjeen, sähkösen, puhelimen tai muun yleisesti käytetyn viestintävälineen avulla Poikkeuksia voidaan tehdä vain oikeuden suostumuksella, lain määrittämässä tapauksissa ja lain mukaisia menettelytapoja noudattaen rikoksen ehkäisemiseksi tai rikostutkintaineiston hankkimiseksi. Viestinnän kuuntelu edellyttää tuomioistuimen myöntämää lupaa. Laittomasti hankittua todistusaineistoa ei voi esittää oikeudessa.

Yrityssalaisuuksien suojaa säännellään Virossa vuodelta 1993 peräisin olevassa kilpailulaissa. (RT I 1993, 47, 642, voimaan 1.1.1994.) Lain 7 § määrittelee yrityssalaisuuden väärinkäytön epäileluksi kilpailuksi, joka on kielletty. Kilpailulaki ei sisällä määräyksiä työntekijöiden velvollisuuksista yrityssalaisuuksien suhteen, vaan nämä velvollisuudet määräytyvät työlaainsäädännön lojaliteettisäännösten perusteella.

Viroon säädettiin ensimmäinen tietosuojalaki vuonna 1996. Nykyinen lainsäädäntö, Viron henkilötietosuojalaki (RT I 2003, 26,158), jolla lainsäädäntö saatetaan henkilötietodirektiivin mukaiseksi, on tullut voimaan 1. lokakuuta 2003 ja sitä on jo muutettu kerran sen jälkeen.

Laki sähköisestä viestinnästä (RT2 I 2004, 87, 593) sisältää luvussa 10 määräykset tietoturvasta ja tietosuojasta.

### *Iso-Britannia*

Iso-Britanniassa perusoikeussäätely perustuu oikeuskäytännön lisäksi Euroopan neuvoston ihmisoikeussopimukseen. Euroopan neuvoston yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi on saatettu Iso-Britanniassa valtiosisäi-

sesti voimaan vuoden 1998 Human Rights Actilla (Human Rights Act 1998). Yksityis- ja perhe-elämä on suojattu sopimuksen 8 artiklassa ja sananvapaus 10 artiklassa.

Yrityssalaisuuksien suoja Iso-Britanniassa perustuu oikeuskäytäntöön ja salassapitosopimuksiin. Henkilötietojen suojasta säädetään vuonna 1998 annetussa Data Protection Actissa, jolla on pantu täytäntöön EU:n henkilötietodirektiivi. Sähköisen viestinnän tietosuojadirektiivi on saatettu voimaan vuonna 2003 Privacy and Electronic Communications (EC Directive) Regulations 2003 (2003 No. 2426) -säännöksellä, jossa on viestintäpalvelujen tarjoajia koskevat säädökset muun muassa tunnistamis- ja paikkatietojen luottamuksellisuudesta sekä sähköisestä suoramarkkinoinnista. Suomessa omaksuttua yhteisötilaajan käsitettä ei Iso-Britanniassa ole käytössä. Säännöksen kohdan 29 mukaan viestintäpalvelun tarjoaja saa käsitellä tietoja, jos se on tarpeen laillisten oikeuksien perustamiseksi, käyttämiseksi tai puolustamiseksi, tai, jos käsittely muuten on tarpeen oikeusprosessiin liittyen. Lisäksi tietoja saa käsitellä jos se on tarpeen rikosten estämiseksi tai selvittämiseksi.

Sähköisen viestinnän luottamuksellisuus perustuu Iso-Britanniassa vuonna 2000 annettuun Regulation of Investigatory Powers Actiin (RIPA). Vuonna 2000 RIPA:n nojalla on annettu säännös Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (2000 No. 2699). Säädös sallii luottamuksellisen viestinnän pääsäännöstä poiketen yritysten ja julkisten tahojen seurata verkossaan tapahtuvaa viestintää myös viestien sisällön osalta muun muassa jonkin seikan toteamiseksi, säädösten tai käyttösääntöjen noudattamisen varmistamiseksi, kansallisen turvallisuuden vuoksi, rikosten tutkimiseksi ja estämiseksi tai luvattoman käytön havaitsemiseksi.

Viestintäverkon ylläpitäjän tulee ilmoittaa verkon käyttäjille siitä, että verkon liikennettä voidaan seurata.

#### *Venäjä*

Venäjän perustuslaki on vuodelta 1993. Perustuslain 23 artiklan mukaan jokaisella

on oikeus yksityiselämään, henkilökohtaiseen ja perheen salaisuuksiin sekä henkilökohtaisen kunnian ja maineen ylläpitämiseen. Lisäksi jokaisella on oikeus yksityisyyteen kirjesalaisuuden, puhelin- ja kaapeliliikenteen ja muiden kommunikaatiomuotojen osalta. Poikkeuksia voidaan sallia ainoastaan oikeuden määräyksellä.

Venäjä on liittovaltio, jossa on lainsäädäntöä sekä liittovaltion eli federaation tasolla sekä alueellisella tasolla. Tiedon avoimuuteen ja suojaamiseen liittyvät kysymykset on käytännössä keskitetty liittovaltion tasolle. Keskeinen säännös on vuoden 1995 Venäjän Federaation laki tiedosta, tiedon käsittelystä ja suojaamisesta. Lain viimeisin muutos on astunut voimaan 1.1.2004.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta suojaa tiedonvälityksen vapautta. Sen mukaan puhelinkeskustelujen nauhoittamisen, sähköisen viestinnän tarkastamisen, kirjelähetysten viivyttämisen, tarkastamisen ja takavarikoimisen ja muun puuttumisen tiedonvälityksen salaisuuteen on tapahduttava oikeuden määräyksellä.

Liittovaltion laki yrityssalaisuuksien suojasta (Laki nro N98-FZ, 29.7.2004) sääntelee kaupallisten salaisuuksien käyttöä ja sitä, kuinka tiedon luottamuksellisuus voidaan turvata. Laki määrittelee liike- ja ammattisalaisuuden ainoastaan yleisin termein. Liikesalaisuuden haltijan tulee yksilöidä liikesalaisuutensa. Toisaalta laki luettelee tiedon, jota ei voida missään oloissa pitää yritysalaisuutena ja luetteloi tietoa, jota voidaan tilanteen mukaan pitää yrityssalaisuutena. Tällaista tietoa on mm. työntekijöiden määrä, palkitsemisjärjestelmät, työolot mukaan luettuina turvallisuusjärjestelyt, työperäiset tapaturmat, ammatilliset kuolleisuusluvut, avoimena olevat työpaikat sekä lainrikkomukset.

Venäjän lainsäädännössä turvataan yrityssalaisuuksia myös siviilikoodin ja kilpailulainsäädännön määräyksillä. Venäjän Federaation siviilikoodin artikla 139 määrää, että liike- ja ammattisalaisuudet on suojattu siviilioikeudellisin oikeussuojakeinoin, erityisesti vahingonkorvausvelvollisuuksin. Vahingonkorvausvelvolliseksi voivat joutua liikesalaisuuden haltijan työntekijät sekä kolmas henkilö, joka vastaanottaa luvattomasti tiedon yrityssalaisuudesta. Mainitun siviilikoodin artiklan

mukaan tiedolla tulee olla todellinen tai mahdollinen kilpailullinen arvo. Toiseksi tiedon tulee olla tuntematon ulkopuolisille sekä yleisesti lain sallimien informaatiokanavien saavuttamattomissa. Kolmanneksi tiedon omistajan tulisi suorittaa toimenpiteitä suojatakseen tiedon luottamuksellisuutta. Muussa tapauksessa tiedon omistaja ei voi näyttää, että tieto on yrityssalaisuus.

Yrityksen on lainsäädännön mukaan tehtävä useita toimia saadakseen tiedolle yrityssalaisuuden aseman. Yrityksen on lueteltava organisaation liikesalaisuuksien piiriin kuuluva aineisto, yrityksen on rajoitettava pääsyä liikesalaisuuteen luomalla menettelyt kyseisen tiedon käsittelyä ja menettelyn noudattamisen valvontaa varten. Yrityksen on myös lueteltava henkilöt, joilla on pääsy kyseiseen tietoon. Sen lisäksi yrityksen on säänneltävä suhdetta liikesalaisuustiedon käyttöön. Työntekijöiden osalta tämä tapahtuu työsopimusten ja liikekumppanien osalta liikesopimusten avulla. Liikesalaisuustieto on lisäksi varustettava tiedon omistajan osoittavalla leimalla.

Venäjän lain mukaan henkilöstön on noudatettava työnantajan asettamia luottamuksellisuusmääräyksiä. Henkilökunnan jäsen ei myöskään saa paljastaa työnantajan liikesalaisuutta aikana, joka on määritelty työnantajan kanssa sopimuksessa työsuhteen kestäessä, tai kolmena työsuhteen päättymisen jälkeisenä vuotena, milloin sopimusta ei ole solmittu. Työntekijän on myös korvattava työnantajalle vahinko, jonka tämä on kärsinyt työntekijän luovuttaessa tietoonsa tulleita yrityssalaisuuksia. Venäjän työsopimuslaki sisältää täsmällisempiä määräyksiä työntekijän korvausvelvollisuudesta ja rangaistusvastuusta. Yrityssalaisuuksien suojaa koskeva laki sisältää kuitenkin määräyksen, jonka mukaan työntekijän on korvattava vahinko, joka on syntynyt työntekijän paljastettua liikesalaisuuksia ulkopuolisille. Työsuhteen päättyessä työntekijän on luovutettava työnantajalle kaikki liikesalaisuuksia sisältävä aineisto. Työnantajan on puolestaan tiedotettava työntekijöille yrityssalaisuuksista, työntekijän velvollisuuksista ja rikkomuksista seuraavista sanktioista.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta sääntelee myös henkilötietoja yleisellä tasolla, vaikka Venäjä ei olekaan

mukana Euroopan neuvoston tietosuojayleissopimuksessa. Henkilöön liittyvät tiedot katsotaan luottamukselliseksi tiedoksi. Henkilötiedot eli tieto kansalaisista tarkoittaa tietoja tosiseikoista, tapahtumista ja elämäntavoista, jotka yksilöivät yksittäisen kansalaisen. Kyseisen lain mukaan luonnollisen henkilön yksityiselämään liittyvän tiedon kerääminen, säilyttäminen, käyttö, levittäminen samoin kuin henkilökohtaiseen tai perhesalaisuuteen liittyvän tiedon käsittely ilman henkilön suostumusta on kielletty, ellei kyse ole tiedon käsittelystä oikeuden määräyksen perusteella tai asianomainen henkilö on antanut suostumuksensa toimenpiteeseen. Samoin viestintäsalaisuutta loukkaavan tiedon kerääminen, säilyttäminen, käyttö tai levittäminen on sallittu vain erityismääräysten nojalla tai asianosaisen suostumuksin.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta viittaa yksityiskohtaisempaan federaation lainsäädäntöön. Seikkaperäinen tietosuojalaki on edelleen valmisteilla. Näitä koskevat ehdotukset tehtiin vuosina 1998 ja 2000 ja lakiesitys on ollut käsiteltävänä Venäjän duumassa vuoden 2006 aikana. Taustalla on Venäjän pyrkimys ratifioida Euroopan neuvoston tietosuojayleissopimus.

Venäjällä ei toistaiseksi ole sähköisen viestinnän tai työelämän tietosuojalainsäädäntöä.

#### 1.4 Nykytilan arviointi

Sähköisen viestinnän tietosuojalaki mahdollistaa yhteisötilaajille tunnistamistietojen käsittelyn niiden normaalin toiminnan edellyttämässä laajuudessa. Käytännössä eräiden voimassa olevien säännösten soveltaminen on osoittautunut ongelmalliseksi. Erityisesti lain 13 § on osoittautunut muotoilultaan niin suppeaksi, ettei se takaa yhteisötilaajille riittäviä toimintamahdollisuuksia.

Yhteisötilaajien mahdollisuuksissa selvittää ja saattaa esitutkintaan viestintäverkkoihinsa kohdistuneita sähköisen viestinnän avulla tapahtuneita väärinkäytöksiä on ilmennyt vaikeuksia. Lain 13 §:n väärinkäytössäädöksen soveltaminen yhteisötilaajien viestintäverkkojen väärinkäytök-

siin on osoittautunut epäselväksi. Voimassa olevan lain ei ole katsottu sallivan yhteisötilaajien kerätä väärinkäytöksistä itse näyttöä, eikä televalvontakaan ole useimmissa tapauksissa ollut käytettävissä.

Sähköisen viestinnän avulla toteutettujen väärinkäytösten selvittämisessä ja esituskintaan saattamisessa on ilmennyt ongelmia, joita ei lakia säädettäessä osattu ennakoida. Myös teleyritykset ovat suhtautuneet varovaisesti säännösten tulkintaan. Tämän lisäksi ongelmia on saattanut syntyä siitä, että toimijoilla ovat menneet lain tarkoittamat viestinnän osapuolen, teleyrityksen ja yhteisötilaajan roolit sekaisin.

### 1.5 Keskeiset ehdotukset

Esityksessä ehdotetaan muutoksia sähköisen viestinnän tietosuojalakiin. Ehdotuksella esitetään laajennettavaksi yhteisötilaajien oikeuksia käsitellä tunnistamistietoja väärinkäytöstilanteissa.

Sääntelyä ehdotetaan muutettavaksi siten, että yhteisötilaajalla olisi tietyin edellytyksin oikeus käsitellä sähköisen viestinnän tunnistamistietoja viestintäverkkonsa tai palvelunsa sekä maksullisten tietoyhteiskunnan palvelujen luvattoman käytön ja käytöstä aiheutuvien kustannusten sekä yrityssalaisuuden oikeudettoman paljastamisen selvittämiseksi.

Ehdotettu tunnistamistietojen käsittelyoikeus liittyy yhteisötilaajien viestintäverkkojen ja viestintäpalvelujen käytön turvaamiseen ja viestintäverkon kautta tapahtuneen elinkeinotoiminnan kannalta keskeisen yrityssalaisuuden paljastamisen selvittämiseen.

Ehdotetun sääntelyn mukaan ensisijaisena keinona viestintäverkon ja viestintäpalvelun käytön asianmukaisuuden turvaamisessa olisi verkkojen ja palvelujen käyttäjille annetut ohjeet ja niiden noudattamisen automaattisesti tapahtuva seuranta.

Sääntelyssä edellytettäisiin, että verkon ja palveluiden suunniteltu käyttö sekä yrityssalaisuuksien suoja on järjestetty asianmukaisin tietoturva- ja käyttäjähallintotoimenpitein. Ehdotetut tunnistamistietojen käsittelyoikeudet eivät oikeuttaisi yhteisötilaajia saamaan tietoa viestien sisällöistä.

Tunnistamistietojen käsittelyllä yhteisötilaaja ei saisi selville muiden kuin omien

viestintäpalveluidensa kautta lähetettyjen ja vastaanotettujen viestien tunnistamistiedot. Kaupallisesti tarjolla olevien sähköposti-, verkkopankki- tai muiden teknisesti suojattujen palveluiden käytöstä tunnistamistiedot paljastaisivat vain palvelun käytön ajankohdan ja keston.

Työnantaja-asemassa olevan yhteisötilaajan tulisi ottaa tunnistamistietojen käsittelyyn liittyvät asiat yhteistoimintamenetelyssä käsiteltäviksi ja tiedottaa niistä työntekijöille.

Ehdotettujen muutosten mahdollistamaa tunnistamistietojen käsittelyä valvoisi tietosuoja-valtuutettu.

## 2 Esityksen vaikutukset

### 2.1 Taloudelliset vaikutukset

Esityksellä voidaan arvioida olevan positiivisia taloudellisia vaikutuksia yhteisötilaajille, viranomaisille ja kuluttajille. Selkeät ja yksiselitteiset käsittelysäännöt ja tiedonsaantia koskevat säännökset vähentävät tarpeettomia prosesseja ja säästävät kaikkien toimijoiden resursseja. Esityksen taloudelliset vaikutukset kohdistuvat lähinnä yrityksiin ja muihin yhteisöihin.

Yritykset ja muut organisaatiot yhteisötilaajina soveltavat sähköisessä viestinnässään lain tunnistamistietojen käsittelysäännöksiä. Käsittelysäännökset ovat mahdollistaneet yhteisötilaajille viestinnän luotamuksellisuudesta huolimatta oikeuden käsitellä käyttäjien tunnistamistietoja ja samalla on turvattu käyttäjien yksityisyyden suoja uutta viestintäteknologiaa käytettäessä. Lain velvoitteiden selväpiirteisyys suomalaisten yritysten ja yhteisöjen aseman kannalta on olennaista.

Tunnistamistietojen käsittelyoikeuksien selkeyttäminen poistaa tulkintaepäselvyyksiä. Uuden 13 a §:n mukainen tunnistamistietojen käsittelyoikeus luvattoman käytön havaitsemiseksi ja lopettamiseksi antaisi yhteisötilaajille aiempaa paremmat mahdollisuudet torjua viestintäverkkojensa ja -palvelujensa luvattonta käyttöä. Samoin kustannuksia aiheuttavien palvelujen luvattonta käyttöä voitaisiin tehokkaasti ehkäistä ja selvittää.

Ehdotetut muutokset parantavat yhteisötilaajien mahdollisuuksia varmistaa vies-

tintäverkkojensa ja palvelujensa käyttö suunnitellulla tavalla elinkeinotoiminnan tukena.

Esityksellä parannettaisiin yhteisötilaajien toimintamahdollisuuksia yritysalaisten suojaamiseksi. Esiitetty muutos on tarpeen teknologisen tai muun kehittämistyön sekä yrityksen liiketoiminnan kannalta keskeisten yritysalaisten tehokkaan suojan varmistamiseksi. Yhteisötilaaja saisi uuden 13 b §:n mukaan käsitellä tunnistamistietoja kun on perusteltua syytä epäillä jonkun lähettäneen tai antaneen oikeudetta pääsyn yritysalaistietoihin. Säännöksellä parannettaisiin tietopääoman omistajan yksinomaista oikeutta omaisuuteensa ja oikeutta hyödyntää omaisuuttaan taloudellisesti. Ehdotettu uudistus turvaisi myös aiempaa paremmin mahdollisuuden turvata esimerkiksi tuotekehitystyön jatkuminen tietovuodoista huolimatta, kun yhteisötilaaja voisi rajata olennaisesti tietovuodosta epäiltyjen piiriä.

Merkittävimmät esityksen taloudelliset vaikutukset kohdistuisivat yritysten toimintaedellytysten turvaamiseen. Yhteisötilaajien mahdollisuudet kehittää toimintaansa, torjua yritystietoon ja tietoverkkoihin kohdistuvaa rikollisuutta ja ylläpitää tietoturvaa paranevat. Samalla sähköisiä palveluja käyttävien kuluttajien asema paranee ja lakia valvovien viranomaisten asema helpottuu.

Esietyt yhteisötilaajien velvollisuudet tunnistamistietojen käsittelyoikeutta käytettäessä aiheuttaisivat yrityksille ja muille organisaatioille jonkin verran kustannuksia, jos he haluavat käyttää ehdotettuja oikeuksiaan. Kustannukset aiheutuisivat henkilöstön koulutuksesta sekä hallinnollisen työn lisääntymisestä huolehdittaessa ehdotettujen 13 c ja 13 d §:n mukaisista velvoitteista.

Ehdotus tarjoaa paremmat edellytykset sähköiselle kaupankäynnille ja asioinnille, joilla on kustannus- ja kilpailukykyvaikutusten vuoksi merkitystä taloudelliselle kehitykselle kotimaassa, yritysten kilpailukyvyille, sisämarkkinoiden ja siten koko eurooppalaisen hyvinvointiyhteiskunnan kehitykselle.

## 2.2 Vaikutukset viranomaisten toimintaan

Ehdotuksen mukaan tietosuojavaltuutettu valvoisi yhteisötilaajien tunnistamistietojen käsittelyä väärinkäytöstilanteissa, joita ovat luvaton käyttö ja yritysalaisuuden oikeudeton paljastaminen.

Ehdotus ei lisäisi valvontaviranomaisen tehtäviä tavalla, jolla olisi vaikutuksia valtiontalouteen, koska valvova viranomainen voi kohdentaa resurssejaan jossain määrin uudelleen. Säännösten täsmentäminen antaisi tietosuojavaltuutetun työlle selkeämmät puitteet, mikä tehostaisi myös lain valvontaa ja sen tavoitteiden toteutumista.

## 2.3 Yhteiskunnalliset vaikutukset

Täsmentämällä viestinnän eri osapuolten oikeuksia ja velvollisuuksia parannetaan erityisesti kuluttajien ja yritysten yleistä luottamusta sähköiseen viestintään ja tätä kautta sähköiseen liiketoiminta- ja asiointiympäristöön kokonaisuudessaan.

Nopea teknologinen kehitys ja verkottuneiden tietoteknisten välineiden laaja levinneisyys on samalla tuonut mukanaan myös uusia riskejä ja mahdollisuuksia laimauttaa yhteiskunnan keskeisiä toimintoja tietoverkkojen avulla. Näissä olosuhteissa tietoturvan merkitys ja sitä koskevan sääntelyn ajankohtaisuus vain korostuu.

Yritysten ja muiden yhteisötilaajien toimintamahdollisuudet paranisivat ehdotuksen myötä ja sääntely mahdollistaisi aiempaa paremmin yhteisötilaajien järjestelmien käytettävyydestä ja tietoturvasta huolehtimisen samalla, kun yksityisyyden suojaa koskevat lain alkuperäiset tavoitteet tulisivat täytetyiksi. Ehdotetut menettelylliset vaatimukset varmistaisivat viestintäverkkojen ja palvelujen käyttäjien yksityisyyden ja viestinnän luottamuksellisuuden. Yritysalaisten suojan parantaminen lisäisi yritysten toimintamahdollisuuksia ja edistää osaltaan taloudellista kehitystä ja hyvinvointia. Yritysten toimintamahdollisuuksien parantaminen kotimaassa edesauttaisi niiden toimintaa myös kansainvälisessä ympäristössä ja kilpailussa.

Ehdotus tarjoaa paremmat edellytykset sähköiselle kaupankäynnille ja asioinnille, joilla on kustannus- ja kilpailukykyvaikutusten vuoksi merkitystä taloudelliselle ke-

hitykselle kotimaassa, yritysten kilpailukyvyille, sisämarkkinoiden ja siten koko eurooppalaisen hyvinvointiyhteiskunnan kehitykselle.

## 2.4 Tietoyhteiskuntavaikutukset

Ehdotettuihin yhteisötilaajan käsittelyoikeuksien edellytyksenä on velvollisuus huolehtia viestintäverkkojen tietoturva, yrityssalaisuuksien suojasta ja laatia viestintäverkkojen ja -palvelujen käytöstä sekä yrityssalaisuuksien käsittelystä ohjeet. Näiden velvollisuuksien voidaan arvioida parantavan pitkällä aikavälillä viestintäverkkojen käytön suunnittelua ja tietoturvariskeiltä suojautumista sekä yritysten toiminnan kannalta tärkeän tietoaineiston suojaamista sähköisessä toimintaympäristössä.

## 2.5 Kansalaisvaikutukset

Ehdotetut yhteisötilaajien tunnistamistietojen käsittelyoikeuksien muutokset vaikuttavat kansalaisten luottamukselliseen viestintään siltä osin, kun yhteisötilaajien viestintäverkkojen ja palvelujen käyttäjät käyttävät yhteisötilaajan viestintämahdollisuuksia omaan viestintäänsä. Käsittelyoikeuksien rajaamisella vakaviin tapauksiin ja niihin liittyvillä menettelyillä on pyritty saamaan aikaan tasapaino viestintäverkkojen ja palvelujen käyttäjien ja yhteisötilaajien oikeutettujen intressien välillä.

Useat yhteisötilaajat ovat myös työnantajia, jolloin heidän tulee ottaa sähköiseen viestintään ja sen seurantaan liittyvät asiat yhteistoimintamenettelyssä käsiteltäviksi ja tiedottaa niistä työntekijöille.

Omaksutun ratkaisun voidaan arvioida mahdollistavan yksityisen viestinnän ja sähköisen asioinnin ja yhteisötilaajien tarpeiden yhteensovittamisen siten että yhteisötilaajat voivat sallia viestintäverkkojensa käytön myös henkilökohtaisiin tarkoituksiin ilman että heidän tarvitsee tinkiä verkon turvallisuudesta.

Tietyissä tilanteissa käyttäjien viestinnän tunnistamistietoja voitaisiin tutkia, mutta missään tapauksessa viestien sisältö ei paljastu ulkopuolisille. Tunnistamistietojen käsittelyyn oikeuttavat tilanteet tulisivat

työntekijöiden tietoon lain menettelysäännösten myötä.

Ehdotetuilla säännöksillä voidaan arvioida olevan myös myönteisiä vaikutuksia viestintäverkkojen ja palvelujen käyttäjien yksityisyyden kannalta, koska verkkojen ja palveluiden tehokkaampi suojaaminen epäasianmukaiselta käyttämiseltä parantaa myös käyttäjiä koskevien tietojen turvallisuutta

## 3 Asian valmistelu

### 3.1 Valmisteluvaiheet ja -aineisto

Esitys on laadittu liikenne- ja viestintäministeriössä.

Sähköisen viestinnän tietosuojalain tulua voimaan vuonna 2004 sen vaikutusten arvioimiseksi perustettiin seurantaryhmä, jossa olivat edustettuina AKAVA ry, Elinkeinoelämän keskusliitto ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Fortum Oyj, Kuluttajavirasto, Keskuskauppakamari ry, liikenne- ja viestintäministeriö, sisäasiainministeriö, Suomen Ammattiliittojen Keskusjärjestö SAK ry, Suomen Suoramarkkinointiliitto ry SSML, Toimihenkilökeskusjärjestö STTK ry, Tekijänoikeuden tiedotus- ja valvontakeskus TTVK ry, Tietosuojavaltuutetun toimisto, työministeriö ja Viestintävirasto. Seurantaryhmässä esiin tulleiden tarpeiden perusteella liikenne- ja viestintäministeriössä valmisteltiin keväällä 2006 luonnos hallituksen esitykseksi muun muassa yhteisötilaajien käsittelyoikeuksien laajentamiseksi.

### 3.2 Lausunnot ja jatkovalmistelu

Luonnos hallituksen esitykseksi lähetettiin lausuttavaksi kaikille ministeriöille ja usealle sadalle eri yhteisölle. Tämän lisäksi hallituksen esitysluonnos saatettiin avoimesti liikenne- ja viestintäministeriön kotisivuille, jotta kaikilla muillakin kuin edellä mainituilla tahoilla oli mahdollisuus lausua asiasta. Lausunnoista on laadittu kokoelma, joka on saatavilla liikenne- ja viestintäministeriön kotisivuilta, osoitteesta [www.mintc.fi/viestintatietoa](http://www.mintc.fi/viestintatietoa).

Lausunnoissa yleisesti kiitettiin lain tämentämistä ja selkeyttämistä. Lausunnoissa kritisoiitiin sitä, ettei lausuntokierroksella olevassa luonnoksessa ollut mukana



vaikutusten arviointia eikä kansainvälistä vertailua. Vaikutusten arviointi valmistui lausuntokierroksen jälkeen. Lausunnot yksittäisiin pykälämuutoksiin olivat vaihtelevia. Tämän johdosta esitykseen tehtiin lausuntokierroksen jälkeen useita muutoksia.

Lausuntokierroksen jälkeen keskeisiltä ministeriöiltä saatiin tehtyihin muutoksiin näkemyksiä.

Liikenne- ja viestintäministeriö pyysi hallituksen esitys luonnoksesta myös oikeuskanslerin lausunnon sen selvittämiseksi, onko hallituksen esityksessä sellaisia ongelmia, jotka estäisivät esityksen antamisen eduskunnan ja sen perustuslakivaliokunnan arvioitavaksi. Oikeuskansleri esitti lausunnossaan näkemyksensä, että esitysluonnoksessa tulisi arvioida kattavammin ja tarvittaessa täydentää luonnosta useiden perusoikeuskysymysten osalta.

Oikeuskanslerin esittämien näkemysten pohjalta esitystä arvioitiin tarpeellisilta osin uudelleen sekä täsmennettiin ja täydennettiin esitystä oikeuskanslerin lausunnossaan esittämällä tavalla.

Esityksen valmistelua jatkettiin liikenne- ja viestintäministeriön 3.10.2006 asettamassa työryhmässä, jonka tehtävänä oli laatia ehdotus sähköisen viestinnän tietosuojalain 13 §:n muuttamiseksi. Ehdotuksessa oli tarkasteltava yhteisötilaajan verkko- ja viestintäpalvelujen tunnistamistietojen käsittelyä 1) luvattoman käytön ja 2) yrityssalaisuuksien paljastamisen tilanteissa. Työryhmän puheenjohtajaksi määrättiin ylijohtaja liikenne- ja viestintämi-

nisteriöstä ja jäseniksi edustajat liikenne- ja viestintäministeriöstä, oikeusministeriöstä, sisäasiainministeriöstä, työministeriöstä, valtiovarainministeriöstä sekä työmarkkinakeskusjärjestöistä.

Esitysluonnoksen tunnistamistietojen käsittelyä koskeviin säännöksiin on työryhmän työn tuloksena lisätty useita merkittäviä täsmennyksiä, jotka kaikki tarkentavat ja asettavat rajoja sekä 13 a ja 13 b §:issä ehdotetulle tunnistamistietojen käsittelylle. Lisäksi esityksen perusteluja ja säätämisyjärjestystä koskevaa arviointia on täydennetty olennaisesti. Esitykseen laadittiin myös kokonaan uusi kansainvälinen vertailu.

### 3.3 Muutosten vaikutusten seuranta

Ehdotettujen muutosten vaikutusten arvioimiseksi liikenne- ja viestintäministeriöön on tarkoitus asettaa seurantaryhmä, jossa olisivat edustettuina ainakin yhteisötilaajien edustajia, Viestintävirasto, tietosuojavaltuutettu, teleyritykset ja työmarkkinakeskusjärjestöt.

Seurantaryhmän toimikausi alkaisi vuoden 2008 kesäkuussa ja kestäisi vuoden 2009 loppuun saakka. Seurantaryhmä teettäisi tutkimukset ehdotetuista maksuerittelysäännösten muutosten vaikutuksista sekä ehdotettujen tunnistamistietojen käsittelyoikeuksien muutosten vaikutuksista yritysten tietohallintoon ja sähköisen viestinnän luottamuksellisuuteen.

## YKSITYISKOHTAISET PERUSTELUT

### I Lakiehdotusten perustelut

#### Sähköisen viestinnän tietosuojalaki

13 a §. *Yhteisötilaajan käsittelyoikeus luvattoman käytön havaitsemiseksi ja lopettamiseksi.* Pykälään otettaisiin säännökset niistä edellytyksistä, joiden rajoissa yhteisötilaaja voi selvittää viestintäverkkonsa ja viestintäpalveluidensa luvattonta käyttöä. Luvattonta

käyttöä olisi sellainen toiminta, jonka yhteisötilaaja on määritellyt luvattomaksi pykälän 2 momentin 2 kohdassa tarkoitetussa ohjeessa.

Yhteisötilaajat voisivat ehdotetun säännöksen nojalla selvittää viestintäverkon, viestintäpalvelun ja tietoyhteiskunnan palvelun luvattonta käyttöä. Ehdotettu tunnistamistietojen käsittelyoikeus liittyy yhteisötilaajien

viestintäverkkojen ja viestintäpalvelujen käytön turvaamiseen.

Ehdotetun sääntelyn mukaan ensisijaisena keinona viestintäverkon ja viestintäpalvelun käytön asianmukaisuuden turvaamisessa olisivat tietoturvasta huolehtiminen sekä verkkojen ja palvelujen käyttäjille annetut ohjeet ja niiden noudattamisen automaattisesti tapahtuva seuranta.

Sähköisen viestinnän tietosuojalain 8 §:n 3 momentin mukaan lain 9–14 §:ssä tarkoitettu tunnistamistietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa ja se on toteutettava luottamuksellisen viestin ja yksityisyyden suojaa tarpeettomasti vaarantamatta. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä.

Lain 8 §:n 3 momentista johtuu, että väärinkäytökset on ensisijaisesti pyrittävä selvittämään muiden kuin luottamuksellista viestintää koskevien tunnistamistietojen avulla. Jos tunnistamistietojen käsittely on välttämätöntä väärinkäytöksen selvittämiseksi, on käsiteltäväksi tulevien tunnistamistietojen piiri rajattava aina tapauskohtaisesti käytettävissä olevien muiden tietojen perusteella.

Ehdotetun säännöksen mukaisia yhteisötilaajan viestintäpalveluja ja tietoyhteiskunnan palveluja olisivat sen omaan viestintäverkkoon liitetyt palvelut sekä sellaiset palvelut, joita käytetään yhteisötilaajan viestintäverkon kautta, mutta jotka ovat luonteeltaan tietoyhteiskunnan palveluja ja joiden käytön yhteisötilaaja maksaa.

Tietoyhteiskunnan palvelujen tarjoamisesta annetun lain (458/2002) 2 §:n mukaan tietoyhteiskunnan palvelulla tarkoitetaan palvelua, joka toimitetaan ilman, että osapuolet ovat yhtä aikaa läsnä, sähköisesti, palvelun vastaanottajan henkilökohtaisesta pyynnöstä tapahtuvana tiedonsiirtona ja tavallisesti vastiketta vastaan.

Lain määritelmän mukaan viestillä tarkoitetaan joko osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa (HE 125/2003 vp, s. 45–46). Tilaajan oikeudesta saada puhelupalvelulaskun erittely on säädetty erikseen. Ehdotettu sääntely ei siten koski

si kiinteän tai matkapuhelinverkon puhelu- palveluita.

Ehdotetussa 1 momentissa säädettäisiin tunnistamistietojen käsittelyn yleisistä edellytyksistä. Momentin mukaan yhteisötilaajan tunnistamistietojen käsittelyoikeus rajattaisiin tilanteisiin, joissa yhteisötilaajalle maksullisia tietoyhteiskunnan palveluja käytetään luvatta taikka viestintäverkkoa tai viestintäpalveluja käytetään viestintäverkon tai viestintäpalvelun käytöstä laadittujen ohjeiden vastaisesti siten, että se on omiaan aiheuttamaan yhteisötilaajalle merkittävää haittaa tai vahinkoa.

Ehdotetussa pykälässä tarkoitettua luvattomasta käytöstä olisi kyse esimerkiksi silloin, jos joku asentaa yhteisötilaajan viestintäverkkoon sen käytöstä annettujen ohjeiden vastaisesti laitteita, ohjelmia tai palveluita tai käyttää muuten viestintäverkkoa tai viestintäpalveluita käytöstä laadittujen ohjeiden vastaisesti.

Esimerkkinä maksullisen tietoyhteiskunnan palvelun luvattomasta käytöstä voisi olla se, että yrityksen henkilökunnan koon mukaan hinnoiteltua palvelua jaettaisiin luvatta ulkopuolisten käyttöön. Tällöin yritys joutuisi vastaamaan hankkimansa käyttöoikeuden ylittävstä käytöstä.

Säännöksessä tarkoitettua merkittävää haittaa voisi muun muassa olla lisääntyneet kustannukset tai sellainen lisääntynyt tiedonsiirtokapasiteetin käyttö, tietoturvausuhka, tai muu vastaava syy, joka vaarantaa, vaikeuttaa, tai hidastaa viestintäverkon tai palvelujen käyttöä niille suunniteltuun käyttötarkoitukseen.

On omiaan -lauseke ilmaisee sen, että yhteisötilaaja voi ryhtyä tunnistamistietojen käsittelyyn myös niissä tilanteissa, joissa luvaton käyttö on havaittu ja kokemusperäisesti arvostellen tiedetään, että se on omiaan aiheuttamaan edellä kuvattuja haitallisia seurauksia, vaikka seuraukset eivät olisi vielä ilmenneet.

Ehdotetussa 2 momentissa säädettäisiin tunnistamistietojen käsittelyn erityisistä edellytyksistä. Momentin 1 kohdan mukaisena tunnistamistietojen käsittelyn edellytyksenä olisi, että yhteisötilaaja on rajoittanut pääsyä viestintäverkkoonsa ja viestintäpalveluunsa ja niiden käyttöön sekä ryhtynyt muihin toimenpiteisiin viestintäverkkonsa ja viestintä-

palvelunsa käytön suojaamiseksi asianmukaisin tietoturvasuostoimenpitein.

Yhteisötilaajan on tullut ennalta käsin asianmukaisesti ryhtyä käytettävissä olevin keinoin toimenpiteisiin sen estämiseksi, että viestintäverkkoa tai siihen liitettyjä palveluja käyttäisivät ulkopuoliset tahot tai sellaiset yhteisötilaajan palveluksessa olevat, joiden käyttöön niitä ei ole osoitettu taikka niitä käytettäisiin käytöstä annettujen ohjeiden vastaisesti. Samoin yhteisötilaajan tulee huolehtia, että tietoturvasuodatus on riittävä. Jos verkkoa tai palveluita asianmukaisesti käyttäjähallinnosta ja muista tietoturva-toimista huolimatta käytetään luvatta, olisi yhteisötilaajalla oikeus tunnistamistietojen käsittelyyn asian selvittämiseksi.

Ehdotetun 2 momentin 2 kohdan mukaisena edellytyksenä on, että yhteisötilaaja on laatinut kirjallisen ohjeen, jossa se on määritellyt, miten sen viestintäverkkoa ja palveluita saa käyttää. Jos yhteisötilaaja haluaa rajoittaa liikennöintiä tai estää liikennöinnin kokonaan tietyn tyyppisiin kohdeosoitteisiin, myös se on määriteltävä ohjeessa. Kohdeosoitteet voitaisiin määritellä kohtuullisen yleisellä tasolla. Määrittelystä tulisi kuitenkin olla selkeästi ymmärrettävissä, mikä on luvaton käyttöä.

Tunnistamistietojen käsittelyn salliminen ehdotetulla tavalla edellyttää, että viestintä-verkon tai viestintäpalvelun käyttäjällä on tieto siitä, miten yhteisötilaajan verkkoa saa käyttää. Noudattamalla näitä vaatimuksia verkon käyttäjä voi välttyä siltä, että hänen viestintäänsä koskevat tunnistamistiedot tulisivat yhteisötilaajan tietoon. On selvää, että ehdotetun 2 momentin 2 kohdassa tarkoitetuissa käyttäjälle annetuissa ohjeissa on oltava riittävän tarkka informaatio viestintä-verkon käytölle asetetuista rajoituksista.

Ehdotetun 3 momentin mukaan yhteisötilaaja saisi käsitellä tunnistamistietoja viestintä-verkon tai viestintäpalvelun luvattoman käytön taikka maksullisten tietoyhteiskunnan palvelujen luvattoman käytön havaitsemiseksi automaattisen hakutoiminnon avulla.

Automaattisella hakutoiminnolla tarkoitetaan toimintoa, jossa hakua ei tapauskohtaisesti kohdisteta ihmistyövoimin, vaan jossa hakukone hakee viestintäverkosta automaattisesti poikkeamia tietyin ennalta määritellyin kriteerein. Automaattinen haku olisi kyseessä

kun viestintäliikennettä analysoidaan masamuotoisesti esimerkiksi liikenteen määrän, tyyppin tai liikenteen kohdeosoitteen tyyppin, mutta ei viestintäverkon tai -palvelun käyttäjän yhteysosoitteen perusteella. Automaattisessa haussa yksittäisen käyttäjän viestien tunnistamistiedot eivät tulisi luonnollisen henkilön tietoon.

Viestintäverkkojen ja viestintäpalvelujen luvaton käyttöä voidaan käytännössä selvittää muun muassa automaattisin kapasiteetin käyttömittarein tai tunkeutumisenestosuvel-luksin, kuten palomuuerein. Samoja teknisiä sovelluksia käytetään myös automaattiseen kapasiteetin seurantaan sekä vika- ja häiriötilanteiden havaitsemiseen. Samoilla sovelluk-silla yhteisötilaajat voivat myös määritellä viestintäverkkonsa ja -palvelunsa käytölle ra-jat: he voivat esimerkiksi estää liikennöinnin omasta verkostaan tiettyihin yhteysosoitteisiin tai estää tietyn tyyppisen liikenteen kokonaan.

Automaattisessa haussa luvaton käyttö tunnistettaisiin viestien koon, tyyppin, määrän, yhteystavan tai viestien kohdeosoitteen pe-rusteella. Viestin tyyppillä tarkoitetaan esi-merkiksi viestin, sen osan tai liitteen tallen-nusmuotoa, kuten esimerkiksi .doc tai .mp3. Viestin yhteystavalla tarkoitetaan esimerkiksi protokollaa, minkä mukaisena se viestintä-verkossa välitetään, kuten http tai tcp. Viestin kohdeosoitteella tarkoitetaan sellaisia palve-luja tai muita osoitteita, joihin suuntautuvaa liikennettä yhteisötilaaja on kieltänyt, rajoit-tanut tai estänyt sen kokonaan.

Edellä mainittujen automaattisen haun määrittelyjen tarkoituksena on, että tunnis-tamistietojen seuranta ei kohdistuisi tavan-omaisiin sähköpostiviesteihin ja että rajoituk-set olisivat muutoinkin asiallisia ja perustel-tuja verkon käytön asiamukaisuuden varmis-tamisen kannalta.

Ennen tunnistamistietojen käsittelyyn ryh-tymistä yhteisötilaajan olisi tullut huolehtia, että kaikki ehdotetussa 1 ja 2 momentissa se-kä 13 c ja 13 d §:ssä tarkoitettut käsittelyn edellytykset täyttyvät.

Ehdotetun 3 momentin mukaan yhteisöti-laaja voisi hakea esille ja ottaa manuaalisesti käsiteltäviksi ne tunnistamistiedot, jotka ovat välttämättömiä asian selvittämiseksi sekä tarvittavien toimien arvioimiseksi.

Manuaalisella käsittelyllä tarkoitetaan säh-köisessä muodossa olevien tietojen käsittelyä

silloin, kun käsittely kohdistetaan ihmistyövoimin tapauskohtaisesti tietyn käyttäjän yhteysosoitteen tai tietyn käyttäjäjoukon yhteysosoitteiden tunnistamistietoihin.

Manuaaliseen käsittelyyn tiedot voisi ottaa *3 momentin 1 kohdan* mukaan automaattisen hakutoiminnon havaittua viestinnässä 1 momentissa tarkoitetuissa tekijöissä poikkeaman. Poikkeamalla tarkoitetaan sellaisia viestejä, joista on niiden koon, tyyppin, määrän, yhteystavan tai kohdeosoitteen perusteella, tallentunut automaattiseen hakuun havainto.

Ehdotetun *3 momentin 2 kohdan* mukaan tunnistamistiedot voisi ottaa manuaalisesti käsiteltäviksi, jos maksullisen tietoyhteiskunnan palvelun epätavallisen korkeiden kustannusten, viestintäverkossa havaitun sinne asennetun palvelun tai muiden näihin rinnastettavien yleisesti havaittavissa olevien seikkojen perusteella on perusteltua syytä epäillä viestintäverkon tai viestintäpalvelun taikka maksullisten tietoyhteiskunnan palvelujen 1 momentissa tarkoitettua luvatonkäyttöä.

Luvatonkäyttöä olisi perusteltua syytä epäillä muun muassa silloin, jos tietohallinnollisen ylläpidon yhteydessä havaitaan viestintäverkossa ilmeisesti oikeudetta asennettu laite tai palvelu. Laitteen tai palvelun oikeudettomuus voisi käydä ilmi esimerkiksi poikkeavasta nimeämisestä tai toiminnallisuudesta. Tällöin voitaisiin selvittää minkälaista liikennettä kyseisestä laitteesta tai palvelusta on tapahtunut.

Lisäksi luvatonkäyttöä voisi olla perusteltu syy epäillä, jos yhteisötilaajan yhteysosoitteesta havaitaan tulevan viestintäpalvelujen määrittäminen nähden vieraan tyyppistä liikennettä tai muun vastaavan seikan perusteella. Esimerkkinä tällaisesta tilanteesta voisi olla se, että yhteisötilaajan verkossa havaitaan sinne luvatta perustettu julkinen verkossa toimiva asunnonvälityspalvelu tai muu yhteisötilaajan toimintaan kuulumaton palvelu.

Ehdotetun säännöksen mukaisessa tunnistamistietojen käsittelyssä on otettava huomioon myös lain 8 §:ssä asetetut rajoitukset, joiden mukaan tunnistamistietojen käsittelyllä ei saa rajoittaa luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä.

Sähköisen viestinnän tietosuojalain 8 § 3 momentin välttämättömyysedellytys asettaa ehdotetulle tunnistamistietojen käsittelylle sekä asialliset että ajalliset rajat. Käsiteltävien tietojen tulisi olla sekä asiallisesti että ajallisesti välttämättömiä 1 momentissa tarkoitettua luvattoman käytön selvittämiseksi ja lopettamiseksi.

Pykälässä ehdotetun tunnistamistietojen käsittelyoikeuden yleisten ja erityisten edellytysten johdosta esimerkiksi työnantaja-asemassa oleva yhteisötilaaja ei voisi seurata viestintäverkon tai viestintäpalvelujen käyttöä työajan seuraamiseksi. Työnantaja ei myöskään voisi seurata työntekijän tavantomaista sähköpostiliikennettä selvittääkseen onko työntekijä ollut yhteydessä esimerkiksi henkilöstön edustajaan, työsuojeluviranomaisiin tai työterveyshuoltoon, koska se ei ole välttämätöntä 1 momentissa tarkoitettua luvattoman käytön selvittämiseksi.

Ajallisesti käsiteltäväksi voitaisiin ottaa vain kulloinkin käsillä olevan tapauksen selvittämisen kannalta välttämättömät tunnistamistiedot eikä säännös oikeuttaisi käsittelemään tunnistamistietoja tätä laajemmin. Luvattoman käytön selvittäminen ei yleensä olisi välttämätöntä ajallisesti kovin pitkään taaksepäin, sillä 1 momentissa tarkoitettujen edellytykset eivät täytyisi. Tosin esimerkiksi maksullisten palvelujen käytön selvittäminen saattaa edellyttää pitempää selvitysjaksoa.

Ehdotettu sääntely ei vaikuta oikeudenkäymiskaaren (4/1734) 17 luvun 24 §:ssä tarkoitettuun lähdesuojaan. Sen mukaan sananvapauden käyttämisestä joukkoviestinnässä annetussa laissa (460/2003) tarkoitettu yleisön saataville toimitetun viestin laatija taikka julkaisija tai ohjelmatoiminnan harjoittaja saa kieltäytyä vastaamasta kysymykseen, kuka on antanut viestin perusteena olevat tiedot, samoin kuin kysymykseen, johon ei voi vastata paljastamatta tietojen antajaa. Sama oikeus on sillä, joka on saanut tiedon edellä mainituista seikoista ollessaan asianomaisen viestin laatijan taikka julkaisijan tai ohjelmatoiminnan harjoittajan palveluksessa. Edellä tarkoitettu henkilö saa kieltäytyä vastaamasta myös kysymykseen, kuka on laatinut yleisön saataville toimitetun viestin, samoin kuin kysymykseen, johon ei voi vastata paljastamatta viestin laatijan henkilöllisyyttä.

Tunnistamistietojen käsittely 13 a ja 8 §:n käsittelysääntöjen vastaisesti saattaa täyttää rikoslain 38 luvun 3 §:ssä ja 4 §:ssä säädetyn viestintäsalaisuuden loukkaamisen tai törkeän viestintäsalaisuuden loukkaamisen tunnusmerkistön.

13 b §. *Yhteisötilaajan käsittelyoikeus yrityssalaisuuksien paljastamisen selvittämiseksi.* Uudessa 13 b §:ssä ehdotetaan säädettäväksi yhteisötilaajan käsittelyoikeudesta epäiltäessä yrityssalaisuuksien oikeudetonta paljastamista.

Ehdotettu tunnistamistietojen käsittelyoikeus liittyy yhteisötilaajien yrityssalaisuuksien oikeudettoman paljastamisen selvittämiseen.

Ehdotetun sääntelyn mukaan ensisijaisina keinoina yrityssalaisuuksien luottamuksellisuuden turvaamisessa olisivat tietoturvasta huolehtiminen sekä verkkojen käyttäjille annetut ohjeet ja niiden noudattamisen automaattisesti tapahtuva seuranta.

Yrityssalaisuuksien oikeudettoman paljastamisen selvittämisessä ovat käytettävissä tietohallinnolliset keinot, kuten käyttäjätietolokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näistä tiedoista käy ilmi, kuka on tallentanut mitään tietoja, missä muodossa, koska ja mille tallenteelle, kuten kovalevylle tai siirrettävälle tallenteelle. Siirrettäviä tallenteita ovat esimerkiksi muistitikut ja cd-levyt. Myös aineiston muuta käsittelyä, kuten tulostamista koskevat tiedot, voidaan tallentaa. Näiden tietojen käsittelylle sähköisen viestinnän tietosuojalaissa ei aseteta rajoituksia. Toisaalta näiden tietojen avulla pystytään vain poikkeuksellisesti selvittämään yrityssalaisuuden paljastaminen kokonaisuudessaan.

Työnantaja voi suojata yrityssalaisuuksia myös muilla tietoturvaluustoimenpiteillä. Esimerkkinä voidaan mainita, että työnantajat käyttävät myös työntekijän kanssa tehtäviä salassapitosopimuksia keinoina yrityssalaisuuksien suojaamisessa. Työnantaja voi myös turvallisuusselvityksistä annetun lain (177/2002) mukaan hankkia selvityksen työntekijän luotettavuudesta, milloin suojattavana on huomattavan arvokas liike- tai ammattisalaisuus tai muu tähän rinnastettava erittäin merkittävä yksityinen etu.

Sähköisen viestinnän tietosuojalain 8 §:n 3 momentin mukaan lain 9–14 §:ssä tarkoitettu tunnistamistietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa ja se on toteutettava luottamuksellisen viestin ja yksityisyyden suojaa tarpeettomasti vaarantamatta. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä.

Ehdotetussa 1 momentissa säädettäisiin tunnistamistietojen käsittelyn yleisistä edellytyksistä. Momentin mukaan yhteisötilaajan tunnistamistietojen käsittelyoikeus kohdistuisi sellaisten viestien havaitsemiseen viestintäverkoissa tai viestintäpalveluissa, jotka voivat johtua siitä, että joku on lähettänyt luvatta tai antanut luvatta pääsyn elinkeinotoiminnan kannalta keskeisiin yrityssalaisuuksiin tai teknologisen tai muun kehittämistyön tuloksiin, jotka ovat tai voivat olla merkittäviä elinkeinotoiminnan käynnistämisen tai harjoittamisen kannalta.

Pykälässä tarkoitettu yrityssalaisuuden käsite vastaisi rikoslain 30 luvun 11 §:n yrityssalaisuuden määritelmää. Rikoslain 30 luvun 11 §:n yrityssalaisuuden määritelmän mukaan yrityssalaisuudella tarkoitetaan liike- tai ammattisalaisuutta, taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle.

Rikoslaisa määritelty yrityssalaisuus on siten jossain määrin laajempi kuin viranomaisen toiminnan julkisuudesta annetun lain (621/1999) elinkeinotoiminnan intressien suojaamiseksi säädetyn salassapitosäännöksen (24 §:n 1 momentin 20 kohta) soveltamisala, jonka piiriin eivät esimerkiksi kuulu elinkeinonharjoittajan velvollisuuksia ja niiden hoitamista koskevat tiedot. Käsite kattaa sellaisetkin teknologista ja muuta kehittämissiivätyötä koskevat tiedot, joissa ei vielä ole kysymys esimerkiksi patentoitavista tuotteista. Yrityssalaisuuden käsitteen piiriin kuuluvat siten myös sellaiset tiedot, jotka viranomaisen toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 21 kohdan mukaan ovat salassa pidettäviä.

Yrityssalaisuuden käsite on katsottu esitystä valmisteltaessa asianmukaisimmaksi käsitteeksi, koska tähän käsitteeseen liittyy kiinteästi elinkeinonharjoittajan oma salassapitoahtaus ja koska säännökset vaikuttavat yksityisten osapuolten välillä.

Tunnistamistietojen käsittely olisi mahdollista silloin, kun kyseessä olisivat elinkeinotoiminnan kannalta keskeiset yrityssalaisuudet taikka teknologisen tai muun kehittämistyön tulokset. Säännöksessä tarkoitettulla tavalla keskeisiä yrityssalaisuuksia olisivat muun muassa tiedot, jotka antavat yritykselle kilpailuedun ja joita ei julkisista lähteistä ole selvitettävissä. Keskeisinä voitaisiin pitää niitä tietoja, joiden käsittelystä ja suojaamisesta elinkeinonharjoittaja on laatinut erityiset ohjeet ja suojaamiskäytännöt kuten 2 momentin 1 ja 2 kohdassa edellytetään.

Kehittämistyön tulokset on mainittu säännöksessä erikseen, koska kaikissa tapauksissa ei ole selvää, missä vaiheessa niitä olisi pidettävä liiketoiminnan kannalta keskeisinä. Kehittämistyön tuloksina voidaan pitää myös tutkimus- tai kehittämishankkeiden sellaiseen merkityksellisiin välivaiheen tuloksia sekä tuloksia, jotka osoittavat kehittämistyön jatkamisen kannattamattomuuden. Tunnistamistietojen käsittelyoikeus esitetään ulotettavaksi tilanteisiin, joissa epäillään kehittämistyön tulosten oikeudetonta paljastamista. Tietojen tulisi olla tai niiden olisi voitava olla merkittäviä elinkeinotoiminnan harjoittamisen tai käynnistämisen kannalta.

Kehittämistyön tulosten oikeudeton paljastaminen voi olla niiden haltijan kannalta erittäin haitallista ja estää muun muassa immateriaalioikeudellisen suojan saamisen.

Ehdotetussa 2 momentissa säädettäisiin tunnistamistietojen käsittelyn erityisistä edellytyksistä. Momentin mukaan käsiteltäväksi voivat tulla vain sellaisten henkilöiden tunnistamistiedot, joille yhteisötalaja on antanut pääsyn tai joilla muutoin on yhteisötalajan hyväksymällä tavalla pääsy yrityssalaisuuksiin. Pääsyn antaminen voi tapahtua esimerkiksi käyttäjäoikeuksia hallinnoimalla. Henkilötahoja, joilla on pääsy yrityssalaisuuksiin, ovat ensisijaisesti asiantuntija- ja kehitystehtävissä työskentelevät henkilöt, joiden tehtäviin yrityssalaisuuksien käsittely kuuluu. Lisäksi yrityssalaisuudet voivat tulla erilaisissa avustavissa tehtävissä työskentelevien sekä

tietojärjestelmien ylläpidosta ja huollosta vastaavien henkilöiden tietoon työtehtävien tai laajojen käyttäjäoikeuksien kautta.

Momentin 1 kohdassa edellytetään, että yrityssalaisuudet olisi tosiasiallisesti suojattava yrityssalaisuuden käsittelyn kannalta ulkopuolisilta tahoilta. Yhteisötalajan on ennen tunnistamistietojen käsittelyn aloittamista tullut rajoittaa pääsyä keskeisiin yrityssalaisuuksiin ja ryhtyä muihin toimenpiteisiin tietojen suojaamiseksi asianmukaisin tietoturvallisuustoimenpitein. Käytännössä tämä tarkoittaa sitä, että organisaatiossa vain tiettyjä tehtäviä hoitavat käyttäjät pääsevät yrityssalaisuuksiin käsiksi. Pääsyä voidaan käytännössä rajoittaa muun muassa tietohallinnollisin toimenpitein, kuten käyttäjätunnukset ja salasanoja tai muuten käyttäjäoikeuksia hallinnoimalla.

Momentin 2 kohdan mukaan yhteisötalajan tulee määritellä, miten yrityssalaisuuksia saa siirtää, luovuttaa tai muutoin käsitellä sähköisessä tietoverkossa sekä laatia tästä kirjallinen ohje, joka on annettava niille viestintäverkon tai viestintäpalvelun käyttäjille, joiden tehtäviin yrityssalaisuuksien käsittely kuuluu. Yrityssalaisuutena suojattavan tiedon kanssa tekemisiin joutuvien olisi mielletävä tieto salaiseksi, mikä ilmenisi rajoitetusta pääsystä ja erityisistä tietojen suojaamistoimista sekä käsittelysäännöistä. Jos yhteisötalaja haluaa kieltää liikennöinnin kokonaan tietyn tyyppisiin kohdeosoitteisiin, myös se on määriteltävä ohjeessa.

Ehdotetun 3 momentin mukaan yhteisötalaja saisi käsitellä tunnistamistietoja automaattisen hakutoiminnon avulla. Automaattisella hakutoiminnolla tarkoitetaan samoja toimintoja kuin 13 a §:n yhteydessä

Ehdotetun 3 momentin mukaan yhteisötalaja voi hakea esille ja ottaa manuaalisesti käsiteltäväkseen ne tunnistamistiedot, jotka ovat välttämättömiä yrityssalaisuuden paljastamisen ja siitä vastuussa olevan selvittämiseksi. Manuaalinen käsittely on yksityiskohtaisesti selvitetty 13 a §:n yksityiskohtaisissa perusteluissa.

Tiedot voisi ottaa manuaalisesti käsiteltäviksi momentin 1 kohdan mukaan automaattisen hakutoiminnon havaittua tietoliikenteessä poikkeaman tai momentin 2 kohdan mukaan, jos yleisesti havaittavissa olevien seikkojen perusteella on perusteltua syytä

epäillä, että yrityssalaisuus on annettu luvattomasti ulkopuoliselle.

Automaattisen haun viestinnässä havaitsemat poikkeamat on selvitetty 13 a §:n yksityiskohtaisissa perusteluissa. Perusteltu syy epäillä yrityssalaisuuksien oikeudetonta paljastamista voisi olla esimerkiksi silloin, jos yrityssalaisuus on julkaistu tai salaisen kehitystytöjen tietojen perusteella joku muu on kehittänyt kehitystyötä harjoittavan tahon kanssa samanlaisen laitteen tai palvelun.

Ehdotettu sääntely ei vaikuta oikeudenkäymiskaaren (4/1734) 17 luvun 24 §:ssä tarkoitettuun lähdesuojaan. Sen mukaan sananvapauden käyttämisestä joukkoviestinnässä annetussa laissa (460/2003) tarkoitettu yleisön saataville toimitetun viestin laatija taikka julkaisija tai ohjelmatoiminnan harjoittaja saa kieltäytyä vastaamasta kysymykseen, kuka on antanut viestin perusteena olevat tiedot, samoin kuin kysymykseen, johon ei voi vastata paljastamatta tietojen antajaa. Sama oikeus on sillä, joka on saanut tiedon edellä mainituista seikoista ollessaan asianomaisen viestin laatijan taikka julkaisijan tai ohjelmatoiminnan harjoittajan palveluksessa. Edellä tarkoitettu henkilö saa kieltäytyä vastaamasta myös kysymykseen, kuka on laatinut yleisön saataville toimitetun viestin, samoin kuin kysymykseen, johon ei voi vastata paljastamatta viestin laatijan henkilöllisyyttä.

Tunnistamistietojen käsittely 13 b ja 8 §:n käsittelysääntöjen vastaisesti saattaa täyttää rikoslain 38 luvun 3 §:ssä ja 4 §:ssä säädetyn viestintäsalaisuuden loukkaamisen tai törkeän viestintäsalaisuuden loukkaamisen tunnusmerkistön

13 c §. *Yhteisötilaajan velvoitteet käsittely-oikeutta käytettäessä.* Uudessa 13 c §:ssä ehdotetaan säädettäväksi kootusti yhteisötilaajan velvoitteista 13 a ja 13 b §:ssä tarkoitetuissa tilanteissa. Pykälä sisältäisi velvoitteita, jotka tulee täyttää ennen käsittelyn aloittamista sekä käsittelyn jälkeen täytettäviä velvoitteita.

Ehdotetun 1 momentin mukaan 13 a ja 13 b §:ssä tarkoitettujen tunnistamistietojen käsittelyn edellytyksenä on se, että yhteisötilaaja on nimennyt ne yhteisötilaajan viestintäverkon ja viestintäpalvelun ylläpidosta ja tietoturvas- ta sekä yhteisötilaajan turvallisuudesta huolehtivat henkilöt, joiden tehtäviin tunnistamistietojen käsittely kuuluu tai määritellyt

mainitut tehtävät. Käyttäjien oikeusturvan kannalta on tärkeää, että he tietävät, ketkä yhteisötilaajan puolesta tunnistamistietoja voivat käsitellä. Yhteisötilaajan tulisi ainakin määritellä ne tehtävät tai esimerkiksi toimintayksiköt, joissa tunnistamistietoja voidaan 13 a ja 13 b §:ssä tarkoitetuissa tilanteissa käsitellä. Jos yhteisötilaaja hankkii kyseisen palvelun ulkopuoliselta taholta, on riittävää, että on määritelty palveluntarjoajan kyseiset tehtävät tai toiminnot.

Jos tunnistamistietojen käsittelyyn osallistuu ulkopuolisen yrityksen palveluksessa oleva henkilö, tulisi yhteisötilaajan varmistua ennen toimenpiteisiin ryhtymistä siitä, että käsittelyn 13 a–13 d §:ssä säädetty edellytykset täyttyvät.

Ehdotetun 2 momentin mukaan yhteisötilaajan olisi laadittava 13 a ja 13 b §:ssä tarkoitettua tunnistamistietojen manuaalisesta käsittelystä siihen osallistuneiden henkilöiden allekirjoittama selvitys.

Selvityksen tulisi sisältää tieto siitä, onko käsittelyn perusteena ollut 13 a vai 13 b §:ssä tarkoitettu tilanne ja millä perusteella tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty. Ehdotettujen 13 a ja 13 b §:n perusteella manuaaliseen käsittelyyn oikeuttaa joko automaattisessa haussa havaittu poikkeama viestinnässä tai yleisesti havaittavissa oleva seikka. Jos käsittelyyn on ryhdytty automaattisen haun perusteella, olisi selvítettävä, minkä automaattisen hakutoimintoon asetetun hakukriteerin perusteella tunnistamistiedot ovat päätyneet manuaaliseen käsittelyyn. Jos käsittelyyn on ryhdytty yleisesti havaittavissa olevan seikan perusteella, olisi kyseinen seikka ilmoitettava.

Selvityksestä tulisi myös käydä ilmi myös ajankohta, käsittelijät ja käsittelystä päättänyt henkilö.

Selvitys on tarpeen viestintäverkkojen ja palvelujen käyttäjien, tietojen käsittelyyn osallistuneiden ja siitä päättäneen henkilön oikeusturvan kannalta. Jälkikäteen on voitava selvittää, kuka tietoja on käsitellyt, mihin ajankohtaan ja kenen aloitteesta. Tiedoilla voidaan jälkikäteen selvittää mahdollisia väärinkäytöksiä. Selvityksen säilyttämisaajaksi ehdotetaan säädettäväksi kaksi vuotta.

Tietosuojavaltuutetun toimisto on 10. päivänä helmikuuta 2003 antanut ohjeen käyttäjälökiä tietojen käsittelystä henkilötietolain

mukaan. Ohjeen mukaan lokiin tallentuvia tietoja voidaan säilyttää niin kauan kuin rekisteröity voi esittää rikosperusteisia vaatimuksia henkilötietojen käsittelijää tai sivullisia vastaan. Ohjeessa todetaan, että koska henkilötietojen lainvastainen käsittely ja rekisteriin tunkeutuminen ovat kriminalisoituja tekoja, joiden syyteoikeus vanhentuu kahdessa vuodessa, on lokia säilytettävä kahden vuoden ajan, jollei aiemmin ole voitu todeta säilyttämisen perusteen menettäneen merkityksensä. Selvityksistä tai tallennetuista tiedoista muodostuu henkilötietolain tarkoittama henkilörekisteri, jota koskee kaikki henkilötietojen käsittelyä koskevat säännökset, kuten esimerkiksi tarkastusoikeutta (26 §), mutta myös tarkastusoikeuden rajoituksia (27 §) koskevat säännökset.

Ehdotetun 3 momentin mukaan 2 momentissa tarkoitettu selvitys on annettava tiedoksi käyttäjälle heti, kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Saatuaan tiedon tunnistamistietojensa käsittelystä, käyttäjällä on mahdollisuus varmistua toimien lain mukaisuudesta ja kääntyä tarvittaessa tietosuojavaltuutetun tai poliisin puoleen. Jos käyttäjä on työntekijä, voi hän kääntyä myös ammattijärjestönsä puoleen.

Momenttiin ehdotetaan otettavaksi säännös siitä, että viestintäverkon tai viestintäpalvelun käyttäjällä on oikeus lakiin tai sopimuksen perustuvan salassapitovelvollisuuden estämättä luovuttaa selvitys ja sen yhteydessä saamansa tiedot etujaan tai oikeuksiaan koskevan asian käsittelyä varten. Säännös olisi pakottava, eikä siitä voisi poiketa sopimuksella.

Selvitystä ei kuitenkaan olisi tarpeen antaa sellaisille käyttäjille, joiden tunnistamistietoja on käsitelty manuaalisesti siten, että käsittely on ollut massamuotoista, eikä se ole kohdistunut tietyn käyttäjän tunnistamistietoihin.

Ehdotuksessa ei ole säädetty selvityksen tiedoksi antamiselle takarajaa. Selvitys tai tiedot olisi annettava mahdollisimman pian käsittelyn päätyttyä. Käynnissä olevasta esitutkinnasta johtuvat tutkinnalliset seikat tai tähän verrattavissa olevat syyt voisivat oikeuttaa selvityksen tiedoksi antamisen lykkäämistä, kunnes tiedoksianto voidaan tutkintaa vaarantamatta tehdä.

Lain 8 §:n 3 momentin välttämättömyysedellytys rajoittaa osaltaan myös tutkinnallisista syistä johtuvaa selvityksen antamisen lykkäämistä. Käsittelyllä ei saa rajoittaa luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä tavoiteltavan tarkoituksen kannalta. Heti kun epäiltyä väärinkäytöstä on selvitetty riittävästi, on käsittely lopetettava ja siitä on laadittava ja annettava käyttäjälle selvitys.

Ehdotetussa 4 momentissa säädettäisiin yhteisötilaajan velvollisuudesta antaa tunnistamistietojen käsittelystä selvitys tietosuojavaltuutetulle. Ehdotetun 1 kohdan mukaan yhteisötilaajan olisi ennen tunnistamistietojen käsittelyn aloittamista annettava tietosuojavaltuutetulle kertaluonteinen selvitys, josta kävisi ilmi tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt sekä tehtävät, joissa tietoja käsitellään. Näiltä osin selvityksestä tulisi käydä ilmi samat seikat, mitkä 13 d §:n 1 momentin 1 kohdan mukaan on käsiteltävä yhteistoimintamenettelyssä. Selvityksestä tulisi käydä selville myös se, miten yhteisötilaaja tiedottaa näistä seikoista viestintäverkkojen ja palvelujen käyttäjille. Jos selvityksen kohteena olevissa seikoissa tapahtuu olennaisia muutoksia, tulisi muutoksista toimittaa uusi selvitys.

Ehdotetun 4 momentin 2 kohdan mukaan yhteisötilaajan tulisi antaa tietosuojavaltuutetulle vuosittain selvitys, jossa hänen olisi selvitettävä kuluneen vuoden osalta kunkin manuaalisen tunnistamistietojen käsittelykerran osalta, onko käsittelyn perusteena ollut 13 a §:ssä tarkoitettu luvaton käyttö vai 13 b §:ssä tarkoitettu yrityssalaisuuden paljastaminen.

13 d §. *Työnantaja-asemassa olevan yhteisötilaajan ja työntekijöiden velvoitteet käsittelyoikeutta käytettäessä.* Uudessa 13 d §:ssä säädettäisiin työnantaja-asemassa olevan yhteisötilaajan velvoitteista, joita on noudatettava 13 c §:ssä tarkoitettujen velvoitteiden lisäksi.

Yksityisyyden suojasta työelämässä annetun lain (759/2004) 4 §:ssä säädetään, että henkilötietojen kerääminen työhönotossa ja työsuhteen aikana kuuluu yhteistoimintalainsäädännössä tarkoitettujen yhteistoimintamenettelyjen piiriin ja asioiden käsittelystä on säädetty muun muassa yhteistoiminnasta yrityksissä annetussa laissa (334/2007) ja yh-



teistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa (651/1988) sekä yhteistoimintamenettelystä kunnissa annetussa laissa (449/2007).

Työnantajan on myös noudatettava, mitä yksityisyyden suojasta työelämässä annetun lain 21 §:ssä säädetään. Säännöksen mukaan työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö kuuluvat edellä mainitussa yhteistoimintalainsäädännössä tarkoitettujen yhteistoimintamenettelyjen piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista.

Yhteistoiminta- tai kuulemismenettelyn jälkeen työnantajan on määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus ja siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä. Lisäksi on otettava huomioon, että työnantaja-asemassa oleviin yhteisötilaajiin sovelletaan edellä mainitun erityislain muitakin säännöksiä, kuten 6 luvussa tarkoitettuja säännöksiä työnantajalle kuuluvien sähköpostiviestien hakemisesta ja avaamisesta.

Säädösten keskinäisestä suhteesta joutuen asiasta on tarpeen säätää myös sähköisen viestinnän tietosuojalaissa. Sääntelyn tarvetta korostaa lisäksi se, että 13 a ja 13 b §:ssä tarkoitettu tunnistamistietojen käsittely ei kaikissa tapauksissa ole henkilötietolaissa (523/1999) tarkoitettua henkilötietojen käsittelyä.

Pykälän 1 momentin 1 kohdan mukaan työnantajan olisi ensinnä käsiteltävä yhteistoiminnasta yrityksissä annetun lain 4 luvussa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa ja työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa (449/2007) tarkoitettua yhteistoimintamenettelyssä 13 a ja 13 b §:ssä tarkoitettujen yrityksessä sovellettavien menettelyjen perusteet ja käytännöt. Tämä tarkoittaa, että ennen kuin työnantaja ottaa käytäntöön 13 a ja 13 b §:ssä tarkoitettuja

menettelyjä tai niiden muutoksia, olisi niiden perusteista, tavoitteista, tarkoituksesta ja vaikutuksista neuvoteltava niiden työntekijöiden edustajien kanssa, joita asia koskee.

Yhteistoimintamenettelyn piiriin kuuluisivat 13 a §:ssä tarkoitettuun luvattomaan käyttöön liittyvät keskeiset kysymykset, kuten viestintäverkon käytöstä laaditut ohjeet, automaattisen haun toimintaperiaatteet ja millä perusteella luvattoman käytön katsotaan aiheuttavan työnantajalle merkittävää haittaa ja vahinkoa. Yhteisötilaajan tulisi selvittää vastaavat seikat myös 13 b §:ssä tarkoitettujen yrityssalaisuuksien paljastamisen selvittämiseen liittyvät vastaavat kysymykset ja perusteet, joiden pohjalta automaattinen tai manuaalinen käsittely on mahdollista.

Toiseksi yhteistoimintamenettelyssä olisi käsiteltävä ne 13 c §:ssä tarkoitettut tehtävät, joissa tunnistamistietoja voidaan käsitellä.

Tämän lisäksi työnantajan olisi tiedotettava käsitellyistä asioista tekemänsä päätökset työntekijöille tai heidän edustajilleen siten kuin yksityisyyden suojasta työelämässä annetun lain 21 §:ssä säädetään.

Momentin 2 kohdassa säädettäisiin työnantajan velvollisuudesta antaa vuosittainen selvitys 13 a ja 13 b §:ssä tarkoitettua tunnistamistietojen manuaalisesta käsittelystä työntekijöiden edustajille yksityisyyden suojan tehokkaan valvonnan toteuttamiseksi. Selvityksen sisältö vastaisi 13 c §:n 4 momentissa tarkoitettua selvitystä; siitä tulisi käydä ilmi tunnistamistietojen manuaalisten käsittelykertojen määrä vuoden aikana ja niiden perusteet.

Pykälän 2 momentin mukaan työntekijöiden edustajalla, jolle 1 momentin 2 ja 3 kohdassa tarkoitettu selvitys olisi annettava, tarkoitetaan lähtökohtaisesti joko työehtosopimuksen mukaista luottamusmiestä tai työsovimuslain 13 luvun 3 §:ssä tarkoitettua luottamusvaltuutettua. Jos jollakin henkilöstöryhmällä ei ole tällaista edustajaa, edustaisi heitä yhteistoimintalainsäädännössä tarkoitettu yhteistoimintaedustaja tai edustaja. Jos tällaista ei olisi valittu, olisi mainittu selvitys annettava tiedoksi kaikille kyseisen henkilöstöryhmän työntekijöille. Tässä tapauksessa työntekijöillä olisi myös yhteisesti oikeus pyytää selvityksen yksityiskohtaisempaa käsittelyä 1 momentin 3 kohdan mukaisesti.

Osa yhteistoimintamenettelyn tai tiedottamisen piiriin kuuluvista tiedoista ei ole julkisia. Elinkeinotoiminnan jatkumisen ja menettelyjen tarkoituksen kannalta on tärkeää, etteivät tiedot leviä pykälän tarkoitusta laajemmin. Tämän vuoksi pykälän 3 momentissa ehdotetaan, että pykälässä tarkoitettu työntekijöiden edustajan tai työntekijän olisi pidettävä salassa tietoonsa saamat yrityssalaisuuden loukkaukset ja epäilyt yrityssalaisuuden loukkaamisesta.

Salassapitovelvollisuuden piiriin kuuluvaa tietoa ei saisi paljastaa sivulliselle senkään jälkeen, kun henkilö ei enää hoida sitä tehtävää, jossa hän on tiedon saanut. Salassapitovelvollisuus jatkuisi sekä työntekijöiden että heidän edustajiensa osalta koko työsuhteen voimassaoloajan. Rangaistuksesta vaitiolovelvollisuuden rikkomisesta säädettäisiin lain 42 §:ssä.

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:ssä säädetään salassapitovelvoitteista. Ehdotettu säännös olisi osittain päällekkäinen siitä, mitkä tiedot säädettäisiin tässä laissa salassa pidettäviksi. Tämä ei ole tarkoituksenmukaista. Siksi ehdotetaan, että virkamiehen ja muun viranomaisessa toimivan vaitiolovelvollisuudesta olisi voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muualla laissa säädetään.

Ehdotettu salassapitovelvollisuus ei estäisi tietojen antamista lakia valvovalle viranomaiselle.

Ehdotuksessa ei oteta kantaa työsuhteen päättämiseen liittyviin kysymyksiin. Kysymys siitä, milloin luvaton viestintäverkkojen, -palvelujen tai tietoyhteiskunnan palvelujen käyttö tai rikollinen toiminta oikeuttaa työsuhteen päättämiseen, ratkeaa työsopimuslain ja muun työoikeudellisen lainsäädännön perusteella. Työsuhteen päättämistä koskevissa oikeudenkäynneissä työnantaja on velvollinen näyttämään työsuhteen päättämisperusteen olemassaolon. Ehdotukset eivät aiheuttaisi muutoksia näihin periaatteisiin.

13 e §. *Yhteisötilaajan oikeus säilyttää tunnistamistietoja.* Ehdotettuun 13 e §:ään ehdotetaan selventävää säännöstä siitä, että 13 a ja 13 b § ei oikeuta yhteisötilaajaa säilyttämään tunnistamistietoja kauempaa kuin lain mukaan on sallittua.

Lain 8 § 3 momentin mukaan tunnistamistiedot on käsittelyn jälkeen hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään.

Sellaiset tunnistamistiedot, joista on tunnistettavissa luonnollinen henkilö, ovat myös henkilötietolaissa (523/1999) tarkoitettuja henkilötietoja. Henkilötietolaissa omaksutun henkilörekisterin käsitteen vuoksi sellaiset tunnistamistiedot muodostavat henkilötietolaissa tarkoitettua henkilörekisterin, vaikka näitä tietoja ei talletettaisikaan erilliseen tekniseen rekisteriin (henkilötietolaki, 3 §:n 3 kohta).

13 f §. *Yhteisötilaajan oikeus tietojen luovuttamiseen.* Pykälään ehdotetaan otettavaksi säännös, joka oikeuttaisi yhteisötilaajan luovuttamaan ehdotetun 13 a ja 13 b §:n mukaisessa menettelyssä saamansa yhteisötilaajan verkon käyttäjää koskevat tunnistamistiedot poliisille asianomistajana tekemänsä rikosilmoituksen tai tutkintapyyntöön yhteydessä. Säännösehdotuksen muotoilussa on otettu huomioon se, että se oikeuttaisi myös poliisin käsittelemään näin saamia tietoja. Säännös on tarpeen sen mahdollistamiseksi, että yhteisötilaaja voi saattaa rikoksena selvitettäväksi sellaiset tapaukset, joissa voi olla kysymys rangaistavaksi säädetystä teosta, kuten luvattomasta käytöstä tai yrityssalaisuuteen kohdistuvasta rikoksesta.

34 §. *Valvontaviranomaisten vaitiolovelvollisuus.* Ehdotuksella lisättäisiin tietosuojavaltuutetun vaitiolovelvollisuuden piiriin ehdotetussa 13 c §:n 4 momentissa tarkoitettua yhteisötilaajan tunnistamistietojen käsittelystä tietosuojavaltuutetulle annettavat selvitykset.

42 §. *Rangaistussäännökset.* Ehdotuksella lisättäisiin lain rangaistussäännökseen uusi 9 kohta, jolla säädettäisiin rangaistavaksi sähköisen viestinnän tietosuojarikkomuksena 13 a–d §:ssä tarkoitettua tunnistamistietojen käsittelyn lainmukaisuuden takaavien toimenpiteiden laiminlyönti. Yhteisötilaajan tulee täyttää nämä velvoitteet vain jos hän tulee käsittelemään tunnistamistietoja 13 a ja 13 b §:ssä tarkoitettulla tavalla.

Jos yhteisötilaaja ei tule käsittelemään tunnistamistietoja, hänen ei tarvitse myöskään täyttää 13 a–d §:ssä tarkoitettuja velvollisuuksia, eikä niiden toimittamatta jättäminen ole tällöin rangaistavaa.

Ehdotetun 9 kohdan mukaan 13 c §:n 1 momentissa tarkoitettujen tunnistamistietojen käsittelijöiden nimeämisen laiminlyönti, pykälän 2 momentissa tarkoitettujen tunnistamistietojen käsittelystä laadittavan selvityksen jättäminen laatimatta tai sen pykälän 3 momentissa säädetyn tiedoksi antamisen laiminlyönti, pykälän 4 momentissa tarkoitettujen tietosuojavaltuutetulle annettavien selvitysten laiminlyönti olisi rangaistavaa. Samoin rangaistavaa olisi 13 d §:n 1 momentin 1 kohdassa tarkoitettujen yhteistoimintamenettelyn laiminlyönti sekä momentin 2 kohdassa tarkoitettujen työntekijöiden edustajille annettavan selvityksen laiminlyönti.

Tunnistamistietojen lainmukaisuuden takaavien velvoitteiden laiminlyönti olisi rangaistavaa vain tahallisena.

### **Laki yksityisyyden suojasta työelämässä**

2 §. Soveltamisala. Yksityisyyden suojasta työelämässä annetun lain soveltamisalassäänökseen esitetään selventävää viittaussäännöstä sähköisen viestinnän tietosuojalakiin.

21 §. *Yhteistoiminta teknisien menetelmien toteutetun valvonnan ja tietoverkon käytön järjestämisessä.* Yhteistoiminnassa käsiteltäviin asioihin esitetään lisättäväksi sähköisen viestinnän tietosuojalakiin esitettyjen uusien 13 a–13 d §:n edellyttämällä tavalla sähköpostin ja muuta sähköistä viestintää koskevien tunnistamistietojen käsittely. Yhteistoimintamenettelyn ja tiedottamisen piiriin kuuluisivat sähköisen viestinnän tietosuojalain 13 a ja 13 b §:ssä tarkoitettujen viestintäverkkojen ja palvelujen käytöstä ja yrityssalaisuuksien käsittelystä annetut ohjeet, tilanteet, joissa käsittely on mahdollista, automaattisen haun yleiset toimintaperiaatteet ja ne tehtävät, joissa tunnistamistietoja voidaan käsitellä.

Lisäksi pykälään esitetään lisättäväksi viittaus työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annettuun lakiin. Viittaus on tarpeen sen selventämiseksi, että yllä kuvattujen tunnistamistietojen käsittelyyn liittyvien seikkojen ottaminen käsiteltäväksi yhteistoimintamenettelyssä koskee myös kuntia.

### **Laki yhteistoiminnasta yrityksissä**

19 §. *Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsittely.* Pykälän 4 kohtaan esitetään lisättäväksi sähköisen viestinnän tietosuojalakiin esitettyjen uusien 13 a–13 d §:n edellyttämällä tavalla sähköpostin ja muuta sähköistä viestintää koskevien tunnistamistietojen käsittely.

### **Laki yhteistoiminnasta valtion virastoissa ja laitoksissa**

7 §. *Yhteistoimintamenettelyn piiriin kuuluvat asiat.* Pykälän 11 a kohtaan esitetään lisättäväksi sähköisen viestinnän tietosuojalakiin esitettyjen uusien 13 a–13 d §:n edellyttämällä tavalla sähköpostin ja muuta sähköistä viestintää koskevien tunnistamistietojen käsittely.

## **II Voimaantulo**

Ehdotettujen lakien on tarkoitus tulla voimaan 1 päivänä kesäkuuta 2008. Esityksessä esitetään muutettavaksi yhteisötilaajiin kohdistuvaa sääntelyä. Yhteisötilaajille on varattava riittävän pitkä aika henkilöstön kouluttamiseksi ja ohjeistamiseksi sekä tarvittavien menettelyjen läpikäymiseksi.

## **III Suhde perustuslakiin ja sääntämisjärjestys**

Ehdotettuja säännöksiä tulee tarkastella perustuslaissa säädettyjen perusoikeuksien näkökulmasta. Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja henkilötietojen suojasta säädetään tarkemmin lailla. Viestinnän luottamuksellisuus on perustuslain 10 §:n 2 momentin nojalla jokaiselle kuuluva perusoikeus. Momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Kyseiset suojeltavat oikeushyvät eivät kuitenkaan ole ehdottomia, sillä niitä joudutaan tietyissä tilanteissa rajoittamaan muun muassa yksilön tai yhteiskunnan turvallisuuden intressissä. Perustuslain 10 §:n 3 momentin mukaan lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi

välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Nämä mahdollisuudet rajoittaa luottamuksellisen viestin suojaa on perusoikeusuudistuksen yhteydessä tarkoitettu tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54).

Perustuslain 10 §:n 3 momentin lakivaraus on valtuutustyyppinen lakivaraus, joka sisältää samalla lainsäätäjän toimivaltaa rajoittavia säännöksiä. Säännöksessä on annettu lainsäätäjälle valta säätää tavallisella lailla välttämättömiä rajoituksia muun muassa viestintäsalaisuuteen rajoituslausekkeessa mainittujen yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten tutkintaan liittyvässä tarkoituksessa. Rajoitukset ovat lainkohdan sanamuodon mukaan mahdollisia ainoastaan yksilön tai yhteiskunnan turvallisuutta (taikka kotirauhaa) vaarantavien rikosten tutkinnassa. Esimerkkeinä perustuslain 10 §:n 3 momentissa tarkoitetuista yksilön tai yhteiskunnan turvallisuutta vaarantavista rikoksista on perusoikeusuudistusta koskevassa hallituksen esityksessä (s. 54) mainittu huumausainerikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetokset.

Luottamuksellisen viestin suojan ensisijaisena tarkoituksena on perusoikeusuudistuksen esitöiden mukaan suojata luottamukselliseksi tarkoitettujen viestin sisältö ulkopuolisilta. Sääntely antaa kuitenkin turvaa muillekin tällaista viestiä koskeville tiedoille, joilla voi olla merkitystä viestin säilymiselle luottamuksellisena. Esimerkkinä perusteluissa on mainittu puhelujen tunnistamistiedot (HE 309/1993 vp, s. 53).

Lakiehdotuksessa viestinnän luottamuksellisuuteen ja yksityisyyden suojaan liittyvät säännökset ovat ehdotetuissa 13 a–13 e §:ssä, joissa säädettäisiin tunnistamistietojen käsittelystä.

Perustuslain 10 § 3 momentin lakivarauksen suhde viestien tunnistamistietoihin ei vaikuttaisi olevan ehdoton. Valiokunnan viimeaikainen käytäntö viittaa siihen, että oikeutta saada tieto viestin tunnistamistiedoista ei tule arvioida perustuslain 10 § 3 momentin

lakivarauksen vaan perusoikeuksien yleisten rajoittamisedellytysten valossa.

Telemarkkinalain muuttamista koskevassa lausunnossaan perustuslakivaliokunta (PeVL 47/1996 vp) arvioi kysymystä telelaskun maksamiseen velvollisen oikeudesta saada tunnistamistiedot perusoikeuksien yleisten rajoittamisperusteiden valossa. Valiokunta piti laskun maksajan epätäydellisten tunnistamistietojen saamisoikeutta välttämättömänä ja oikeasuhtaisena laskujen maksamisvelvollisuuteen liittyvän tietojensaantitarpeen kannalta. Käsitellessään esitystä laiksi yksityisyyden suojasta työelämässä valiokunta arvioi työnantajan oikeutta selvittää sitä, onko työntekijän sähköpostiosoitteeseen tämän poissa ollessa saapunut tai onko hän välittömästi ennen poissaoloaan lähettänyt tai vastaanottanut työnantajalle tarkoitettuja viestejä, joista työnantajan on toimintojensa järjestämisen tai turvaamisen takia välttämätöntä saada tieto (PeVL 10/2004 vp). Valiokunta katsoi, että työnantajaa ei voitu pitää sellaisena ulkopuolisena tahona jota vastaan perustuslain 10 §:n säännöksillä luottamuksellisen viestin salaisuudesta on tarkoitus antaa suojaa. Valiokunnan mukaan esityksessä ehdotettujen luottamuksellisen viestinnän salaisuuden rajoituksia oli arvioitava perusoikeuksien yleisten rajoitusedellytysten kannalta.

Ehdotetussa sääntelyssä olisi kyse samankaltaisesti tilanteesta, mistä on säädetty laissa yksityisyyden suojasta työelämässä annetussa laissa. Nyt ehdotetussa sääntelyssä ei kuitenkaan annettaisi oikeutta puuttua viestien sisältöön vaan ainoastaan tavallisten postilähetysten osoitetietoja vastaaviin viestien tunnistamistietoihin.

Yhteisötilaaja, joka usein on myös työnantaja, saisi tietyin edellytyksin selvittää perustellun epäilyn siitä, onko hänen viestintäverkkoaan käytetty luvattomasti tai onko sen kautta annettu luvattomasti tieto elinkeinotoiminnan kannalta keskeisistä yrityssalaisuuksista. Yhteisötilaaja ei ole viestintään nähden samalla tavoin ulkopuolinen taho kuin esimerkiksi teleyritys. Yhteisötilaaja tilaa viestintäpalvelut käyttäjiensä, kuten työntekijöiden, käytettäväksi. Yhteisötilaajien osalta viestintäpalveluiden tarjoaminen käyttäjille liittyy hyvin kiinteästi yhteisötilaajan pääasiallisen toiminnan mahdollistamiseen. Yhteisötilaaja ei myöskään saisi tunnistamis-

tietoja ulkopuoliselta taholta, koska tiedot kerääntyvät yhteisötilaajan hallussa oleviin laitteisiin. Näin ollen voitaneen arvioida, että 13 a ja 13 b §:ssä ehdotettua tunnistamistietojen käsittelyoikeutta ei tarvitse sitoa tiettyihin rikostunnusmerkistöihin, vaan mahdollisia rajoituksia viestinnän luottamuksellisuuteen voidaan tarkastella perusoikeuksien yleisten rajoitusedellytysten kannalta.

Ehdotettu sääntely vaikuttaisi yksityisten oikeussubjektien välisessä suhteessa. Tällöin perusoikeusarviossa korostuu perustuslain 22 §:n säädös julkisen vallan velvollisuudesta turvata perusoikeuksien toteutuminen. Tässä olevassa tapauksessa turvaamisvelvollisuus liittyy viestintäpalvelujen käyttäjien ja yhteisötilaajien oikeudet tasapainoisesti yhteen sovittavaan sääntelyratkaisuun. Tämä arvio sisältyy arvioon ehdotettujen muutosten hyväksyttävyydestä perusoikeuksien yleisten rajoitusedellytysten kannalta.

Sähköisen viestinnän tunnistamistietojen käsittelyoikeudesta ehdotetaan säädettäväksi lain tasoisella säädöksellä. Tunnistamistietojen käsittelyyn oikeuttavat tilanteet, käsittelyoikeuden rajat ja käsittelyn lainmukaisuuden varmistavat säännökset ehdotetaan sijoitettaviksi sähköisen viestinnän tietosuojalakiin.

Ehdotetuissa 13 a ja 13 b §:ssä esitetyt muutokset tunnistamistietojen käsittelyoikeuksiin on rajattu koskemaan vain yhteisötilaajien toiminnan kannalta tärkeitä uhkia. Tunnistamistietoja saisi käsitellä automaattisen hakutoiminnon avulla ennakolta määriteltyjen hakuperusteiden perusteella siten, että yksittäisten viestintäverkon käyttäjien viestien tunnistamistiedot eivät tulisi kenenkään ulkopuolisen henkilön tietoon. Tunnistamistiedot saisi ottaa tapauskohtaisesti kohdistettavaan manuaaliseen käsittelyyn vain automaattisessa hakutoiminnossa havaitun poikkeaman tai yleisesti havaittavissa olevan seikan perusteella syntyneen perustellun epäilyn perusteella.

Tunnistamistietojen käsittelyoikeuden edellytyksenä olisi, että viestintäverkon käyttö ja yrityssalaisuuksien luottamuksellisuus olisi ensisijaisesti pyrittävä takaamaan asianmukaisin käyttäjähallinto- ja tietoturvatoinen. Lisäksi viestintäverkon käytöstä ja yrityssalaisuuksien käsittelystä tulisi antaa viestintäverkon käyttäjille kirjallinen ohje.

Ehdotettu 13 a § oikeuttaisi käsittelemään tunnistamistietoja maksullisten tietoyhteiskunnan palvelujen luvattoman käytön tai viestintäverkkoon sen käytöstä laadittujen ohjeiden vastaisesti asennettujen laitteiden, ohjelmien ja palvelujen tai muun näihin rinnastuvan viestintäverkon tai viestintäpalvelun luvattoman käytön havaitsemiseksi, joka on omiaan aiheuttamaan merkittävää haittaa tai vahinkoa. Säännöksessä on pyritty ennakkoimaan tyypillisimmät luvattoman käytön tilanteet. Viestintätekniikan nopean kehityksen vuoksi kaikkia luvattoman käytön tilanteita ei ole mahdollista luetella tyhjentävästi. Tämän vuoksi tunnistamistietojen käsittely säännöksessä tarkoitettuihin esimerkkitapauksiin rinnastettavan muun luvattoman käytön havaitsemiseksi on syytä sisällyttää säännökseen.

Ehdotettu 13 b § antaisi yhteisötilaajille oikeuden tunnistamistietojen käsittelyyn, jos yhteisötilaajan viestintäverkon tai viestintäpalvelun käyttäjä lähettää tai antaa luvatta sivulliselle pääsyn yhteisötilaajan viestintäverkon kautta tai viestintäpalvelua hyväksi käyttämällä yhteisötilaajan tai tämän asiakkaan tai muun yhteistyökumppanin elinkeinotoiminnan kannalta keskeisiin yrityssalaisuuksiin taikka teknologisen tai muun kehittämistyön tuloksiin, jotka ovat tai voivat olla merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta. Käsittelyoikeus kohdistuisi vain sellaisten henkilöiden tunnistamistietoihin, joilla on yhteisötilaajan hyväksymällä tavalla pääsy yrityssalaisuuksiin. Tunnistamistietojen käsittelyn edellytyksenä olisi erityisen yrityssalaisuuksien käsittelyohjeen laatiminen. Näin ollen ehdotettu käsittelyoikeus tulisi sovellettavaksi vain sellaisiin yhteisötilaajiin, joiden normaaliin toimintaan säännöksessä tarkoitettujen yrityssalaisuuksien käsittely kuuluu.

Ehdotetun 13 b §:n yrityssalaisuuden käsite on yhtenevä rikoslain 30 luvun 11 §:n yrityssalaisuuden määritelmän kanssa. Tunnistamistietojen käsittely olisi mahdollista vain jos kyseessä olisivat elinkeinotoiminnan käynnistämisen tai harjoittamisen kannalta keskeiset yrityssalaisuudet tai kehittämistyön tulokset. Säännöksen yksityiskohtaisissa perusteluissa esimerkkeinä on mainittu muun muassa tiedot, jotka antavat yritykselle kilpailuedun ja joita ei julkisista lähteistä ole

selvitettävissä sekä tiedot, joiden käsittelystä ja suojaamisesta elinkeinonharjoittaja on laatinut erityiset ohjeet ja suojaamiskäytännöt. Ehdotetussa säännöksessä rikoslaissa tarkoitettulle yrityssalaisuuden käsitteelle on asetettu rikoslakia korkeampi merkittävyystaso. Rikoslain esitöissä on todettu, että yrityssalaisuuden käsitteen laissa omaksuttua tarkempaan sisällölliseen rajaukseen ei ole tarvetta, koska elinkeinotoiminnassa tarvitaan mitä erilaatuisempaa kilpailijoilta suojattavaa tietoa (HE 66/1988 vp, s. 92). Ehdotettua sääntelyä voitaneen pitää säänneltävä asiakokonaisuus huomioon ottaen tarkkarajaisena.

Perustuslakivaliokunta kiinnitti huomiota sähköisen viestinnän tietosuojalain esityksen yhteydessä käsittelyn määritelmän laaja-alaisuuteen (muun muassa PeVL 9/2004 vp, s. 3/I). Valiokunta totesi kuitenkin, että ehdotuksen 8 § 3 momentin tarkoitussidonnaisuuden vaatimus lieventää laaja-alaiseen käsittelyn määritelmään liittyviä ongelmia. Mainittu 8 §:n 3 momentti rajoittaisi ja ohjaisi myös ehdotettujen säännösten nojalla tapahtuvaa tunnistamistietojen käsittelyä.

Ehdotetulla 13 a § mukaisella tunnistamistietojen käsittelyoikeudella pyritään turvaamaan yhteisötilaajien viestintäverkkojen ja palvelujen käyttö niille suunniteltuun tarkoitukseen. Sähköisten viestintäverkkojen ja palvelujen käytön turvaamisen voitaneen arvioida olevan varallisuusarvoinen etuus, joka nykyisessä viestintäkeskeisessä toimintaympäristössä lukeutuu perustuslain 15 §:ssä säädetyn omaisuudensuojan piiriin.

Ehdotetulla 13 b §:n mukaisella tunnistamistietojen käsittelyoikeudella pyritään suojaamaan teknologisen tai muun kehittämistyön tuloksia ja elinkeinotoiminnan kannalta keskeisiä yrityssalaisuuksia. Yhteisötilaajan elinkeinotoiminnan kannalta keskeisten yrityssalaisuuksien ja kehittämistyön tulosten luottamuksellisuuden varmistamisen voidaan niin ikään arvioida kuuluvan omaisuuden suojan piiriin. Perustuslakivaliokunta on käsitellyt asiaa muun muassa teletoimintalain muuttamisesta (PeVL 1/1996 vp), telemarkkinalain (PeVL 47/1996 vp, PeVL 34/2000 vp ja PeVL 5/2001 vp) sekä viestintämarkkinoita koskevan lainsäädännön (PeVL 8/2002 vp) muuttamisesta annettuja esityksiä käsitellessään.

Valiokunnan tähänastinen käytäntö voidaan tiivistää siten, että omaisuuden suojaan kohdistuvat erilaiset velvoitteet ovat omaisuuden erityisluonne huomioon ottaen perustuslain mukaisia, jos velvoitteet perustuvat lain täsmällisiin säännöksiin ja ovat omistajan kannalta kohtuullisia. Perustuslakivaliokunta on lausuntokäytännössään pitänyt keskeisenä sitä, että omistajan oma nykyinen ja kohtuullinen tuleva tarve rajoittavat omistajalle asetettavia velvollisuuksia.

Viestin tunnistamistietojen on perustuslakivaliokunnan vakiintuneen käytännön mukaan katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (PeVL 47/1996 vp, s. 4/I, PeVL 7/1997 vp, s. 2/I, PeVL 26/2001 vp, s. 3/II, PeVL 9/2004 vp, s. 4/I, PeVL 10/2004 vp, s. 4/II, PeVL 16/2004 vp, s. 6/I, PeVL 23/2006 vp, s. 3/I). Ehdotetut yhteisötilaajien tunnistamistietojen käsittelyoikeuksien muutokset eivät antaisi oikeutta ottaa selville viestien sisältöjä. Pelkkiin viestien tunnistamistietoihin rajautuva käsittelyoikeus ei ulottuisi luottamuksellisen viestin salaisuuden ydinalueelle.

Yhteisötilaajilla on perusteltu tarve turvata viestintäverkkojensa ja viestintäpalveluidensa käyttö niiden oman toimintansa tarpeisiin. Yhteisötilaajilla on myös perusteltu tarve turvata omien ja yhteistyökumppaneidensa yrityssalaisuuksien luottamuksellisuus. Aineeton omaisuus, kuten kehitteillä olevat tuotteet ja palvelut, tietotaitoon perustuvat toimintatavat ja muut yrityssalaisuudet saattavat muodostaa etenkin korkean teknologian yritysten varallisuudesta merkittävän osan.

Ehdotetun sääntelyn mukaan ensisijaisena keinona viestintäverkon ja viestintäpalveluiden suojaamisessa ja yrityssalaisuuksien luottamuksellisuuden turvaamisessa olisi verkkojen käyttäjille annetut ohjeet ja niiden noudattamisen automaattisesti tapahtuva seuranta sekä tietoturva-toimenpiteet.

Viestintäverkkojen ja viestintäpalveluiden ohjeiden mukainen käyttö voidaan turvata vain osaksi tietohallinnollisin toimenpitein. Väärinkäytösten selvittäminen edellyttää kuitenkin myös tunnistamistietojen käsittelyä.

Yrityssalaisuuksien oikeudettoman paljastamisen selvittämisessä ovat niin ikään käytettävissä tietohallinnolliset keinot, kuten käyttäjätietolokien tarkastaminen, pääsyä ra-

joittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näistä tiedoista käy ilmi, kuka on tallentanut mitään tietoja, missä muodossa, koska ja mille tallenteelle, kuten kovalevyille tai siirrettävälle tallenteelle. Siirrettäviä tallenteita ovat esimerkiksi muistitikut ja cd-levyt. Myös aineiston muuta käsittelyä, kuten tulostamista koskevat tiedot, voidaan tallentaa. Näiden tietojen käsittelylle sähköisen viestinnän tietosuojalaissa ei aseteta rajoituksia. Toisaalta näiden tietojen avulla pystytään vain poikkeuksellisesti selvittämään yrityssalaisuuden paljastaminen kokonaisuudessaan.

Sähköisen viestinnän tietosuojalaki ei rajoita yhteisötilaajien mahdollisuuksia turvata omaisuuttaan käyttämällä tietohallinnollisia järjestelmiä, joihin kirjautuu yksityiskohtaiset tiedot siitä, kuka on avannut, muokannut tai siirtänyt sähköisessä muodossa olevia tietoja. Ehdotetun sääntelyn mukaan tunnistamistietojen käsittelyyn voisi turvautua vain jos asianmukaisista suojauskäytännöistä huolimatta yrityssalaisuudet on annettu luvatta ulkopuolisille.

Ehdotettu käsittelyoikeus kohdistuisi yhteisötilaajan omiin palveluihin. Internetissä toimivien suojattujen sähköposti- ja verkkopankkipalveluiden käytöstä selviäisi ainoastaan käytetyn palvelun osoite, käyttämisaika ja käytön kesto. Yhteisötilaajilla on mahdollisuus halutessaan estää ulkopuolisten tarjoamien palvelujen käyttö omista järjestelmistään.

Ehdotettu tunnistamistietojen käsittelyoikeus on välttämätön, jotta yhteisötilaajat voisivat nopeasti selvittää epäilyt viestintäjärjestelmiensä luvattomasta käytöstä ja yrityssalaisuuksien luvattomasta paljastamisesta. Yrityssalaisuuksien osalta tietohallinnollisten toimien avulla pystytään alustavasti rajaamaan epäilyksen alaisten joukkoa selvittämällä ketkä ovat tietoja käsitelleet. Tunnistamistietojen käsittely on välttämätöntä, jotta saadaan tieto siitä, onko joku ollut yhteydessä esimerkiksi tahoon, jolle yrityssalaisuus on luvatta annettu. Samalla yhteisötilaaja pystyisi rajaamaan epäilytjen piiriä ja näin turvaamaan toimintansa jatkumisen.

Ilman ehdotettua käsittelyoikeutta yhteisötilaajat eivät pysty nopeisiin toimenpiteisiin yrityssalaisuuksiin liittyvien väärinkäytösten

havaitsemiseksi ja niiden aiheuttamien vahinkojen torjumiseksi tai rajoittamiseksi.

Ehdotukseen sisältyy useita yhteisötilaajille esitettyjä velvollisuuksia, jotka varmistaisivat tunnistamistietojen käsittelyn lain mukaisuuden ja näin mahdollisimman vähäisen puuttumisen viestinnän luottamuksellisuuteen. Yhteisötilaajien käsittelyoikeuden edellytyksenä on, että viestintäverkot ja viestintäpalvelut on suojattu ulkopuolisilta ja niiden tietoturvasta on huolehdittu. Lisäksi yhteisötilaajan tulee ennalta käsin nimetä ne tehtävät, joissa toimivien tehtäviin tunnistamistietojen käsittely kuuluu. Työnantaja-asemassa olevien yhteisötilaajien tulee ottaa tunnistamistietojen käsittelyssä noudatettavat käytännöt ja viestintäverkon käytöstä annetut ohjeet käsiteltäväksi yhteistoiminta-menettelyssä ja tiedottaa niistä työntekijöille. Ennen tunnistamistietojen käsittelyn aloittamista yhteisötilaajan tulisi toimittaa tietosuojavaltuutetulle selvitys käsittelyssä noudatettavista käytännöistä ja siitä, miten niistä on tiedotettu viestintäverkon käyttäjille.

Tunnistamistietojen manuaalisessa käsittelyssä tunnistamistiedot tulisivat niitä käsittelevien henkilöiden tietoon. Tällaisesta käsitelystä tulisi aina laatia ehdotetun 13 c §:n 2 momentin mukainen käsittelyyn osallistuneiden henkilöiden allekirjoittama selvitys, josta kävisi ilmi käsittelyn peruste ja syy, minkä vuoksi tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty. Selvityksestä olisi lisäksi käytävä ilmi käsittelyn ajankohta, kesto ja käsitelijät sekä käsittelystä päättänyt henkilö. Selvitys tulisi antaa viestintäverkon tai viestintäpalvelun käyttäjälle, heti kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta.

Yhteisötilaajien tulisi myös toimittaa tietosuojavaltuutetulle vuosittain tunnistamistietojen manuaalisesta käsittelystä selvitys, josta kävisi ilmi, montako kertaa tunnistamistietoja on manuaalisesti käsitelty ja millä perusteella käsittelyyn on ryhdytty. Sama tieto tulisi työpaikoilla henkilöstöryhmien edustajille.

Ehdotetun sääntelyn oikeusturvatakeet perustuvat käyttäjien ohjeistukseen, tunnistamistietojen käsittelyn suunnitteluun sekä tietojen antamiseen käyttäjille ja valvovalle viranomaiselle. Koska kyseessä on etupäässä yksityisten välisissä suhteissa tapahtuva toiminta, on tärkeää, että ne, joiden tietoja on

käsitelty, saavat siitä välittömästi tiedon. Tällöin tietojen käsittelyn asianmukaisuus voidaan arvioida tuoreeltaan ja ryhtyä tarvittaessa selvittämään asiaa lakia valvovan tietosuojavaltuutetun tai poliisin avulla. Tietosuojavaltuutetulle ennen tunnistamistietojen käsittelyn aloittamista ja tämän jälkeen vuosittain toimitettavien selvitysten perusteella valvova viranomainen saisi tiedon noudatettavista käytännöistä ja käsittelyn yleisyydestä.

Ehdotetut muutokset ovat Suomea sitovien kansainvälisten ihmisoikeusvelvoitteiden mukaisia. Euroopan neuvoston ihmisoikeussopimus tai Euroopan neuvoston tietosuojasopimus eivät aseta rajoituksia ehdotetuille muutoksille. Myös EY:n sähköisen viestinnän tietosuojadirektiivi sallii ehdotetun kaltaisen sääntelyn. Euroopan neuvoston ihmisoikeustuomioistuimien on ottanut kannan viestinnän seurantaan 3 päivänä huhtikuuta 2007

antamassaan tuomiossa asiassa *Copland v. Yhdistynyt kuningaskunta*. Tapauksessa julkisen oppilaitoksen työntekijän puheluja, sähköposteja ja internetin käyttöä oli seurattu. Toiminnan salliva säädös tuli Yhdistyneessä kuningaskunnassa voimaan tapahtuneen seurannan jälkeen. Ihmisoikeustuomioistuin ei sinänsä sulkenut pois mahdollisuutta, että työntekijän puhelimen, sähköpostin ja internetin käytön valvonta voisi joissakin olosuhteissa olla Euroopan neuvoston ihmisoikeussopimuksessa tarkoitettulla tavalla välttämätöntä demokraattisessa yhteiskunnassa tavoiteltaessa hyväksyttävää päämäärää.

Edellä kerrotuilla perusteilla katsotaan, että lakiehdotus voitaisiin käsitellä tavallisessa lainsäätämisyjärjestyksessä. Toivottavana kuitenkin pidetään, että esityksestä hankitaan perustuslakivaliokunnan lausunto.

Edellä esitetyn perusteella annetaan Eduskunnan hyväksyttäväksi seuraava lakiehdotus



## 1.

**Laki****sähköisen viestinnän tietosuojalain muuttamisesta**

Eduskunnan päätöksen mukaisesti  
*muutetaan 16 päivänä kesäkuuta 2004 annetun sähköisen viestinnän tietosuojalain (516/2004) 34 §:n johdantokappale ja 1 ja 2 momentti sekä 42 §:n 2 momentin 7 ja 8 kohta ja lisätään 13 a–13 f § sekä 42 §:n 2 momenttiin 9 kohta seuraavasti:*

## 13 a §

*Yhteisötilaajan käsittelyoikeus luvattoman käytön havaitsemiseksi ja lopettamiseksi*

Yhteisötilaaja voi jäljempänä tässä pykälässä säädetyn edellytyksin käsitellä tunnistamistietoja maksullisten tietoyhteiskunnan palvelujen luvattoman käytön tai viestintäverkkoon sen käytöstä laadittujen ohjeiden vastaisesti asennettujen laitteiden, ohjelmien ja palvelujen tai muun näihin rinnastuvan viestintäverkon tai viestintäpalvelun luvattoman käytön havaitsemiseksi, joka on omiaan aiheuttamaan merkittävää haittaa tai vahinkoa.

Tunnistamistietojen käsittely on sallittua, jos yhteisötilaaja on ennen käsittelyn aloittamista:

1) rajoittanut pääsyä viestintäverkkoonsa ja viestintäpalveluunsa ja niiden käyttöön sekä ryhtynyt muihin toimenpiteisiin viestintäverkkonsa ja viestintäpalvelunsa käytön suojaamiseksi asianmukaisin tietoturvallisuustoimenpitein; ja

2) määritellyt, minkälaisia viestejä sen viestintäverkon kautta saa välittää ja hakea, sekä miten sen viestintäverkkoa ja viestintäpalvelua saa muutoin käyttää ja minkälaisiin kohdeosoitteisiin viestintää ei saa harjoittaa, sekä laatinut tästä kirjallisen viestintäverkon tai viestintäpalvelun käyttäjälle annetun ohjeen.

Yhteisötilaaja saa käsitellä tunnistamistietoja automaattisen hakutoiminnon avulla. Automaattinen hakutoiminto voi perustua viestin kokoon tai viestien yhteenlaskettuun

kokoon taikka viestien tyyppiin, määrään tai yhteystapaan taikka viestien kohdeosoitteisiin. Yhteisötilaaja voi hakea esille ja ottaa manuaalisesti käsiteltäväksi ne tunnistamistiedot, jotka ovat välttämättömiä luvattoman käytön ja siitä vastuussa olevien selvittämiseksi ja käytön lopettamiseksi, jos:

1) automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama; tai

2) maksullisen tietoyhteiskunnan palvelun kustannukset ovat nousseet epätavallisen korkeiksi, viestintäverkossa havaitaan sinne oikeudetta asennettu laite, ohjelma tai palvelu taikka jos muiden näihin rinnastettavien yleisesti havaittavissa olevien seikkojen perusteella on perusteltu syy epäillä, että viestintäverkkoa, viestintäpalvelua tai maksullisia tietoyhteiskunnan palveluja on käytetty luvottomasti.

## 13 b §

*Yhteisötilaajan käsittelyoikeus yrityssalaisuuksien paljastamisen selvittämiseksi*

Yhteisötilaaja voi jäljempänä tässä pykälässä säädetyn edellytyksin käsitellä tunnistamistietoja sellaisten viestien havaitsemiseksi viestintäverkossaan tai viestintäpalvelussaan, jotka voivat johtua siitä, että yhteisötilaajan viestintäverkon tai viestintäpalvelun käyttäjä lähettää tai antaa luvatta sivulliselle pääsyn yhteisötilaajan viestintäverkon kautta tai viestintäpalvelua hyväksi käyttämällä yhteisötilaajan tai tämän asiakkaan tai muun yhteistyökumppanin elinkeinotoiminnan kanalta keskeisiin yrityssalaisuuksiin taikka

teknologisen tai muun kehittämistyön tuloksiin, jotka ovat tai voivat olla merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta.

Yhteisötilaaja saa käsitellä ainoastaan sellaisten henkilöiden tunnistamistietoja, joille yhteisötilaaja on antanut tai joilla muutoin on yhteisötilaajan hyväksymällä tavalla pääsy yrityssalaisuuksiin. Tunnistamistietojen käsittely on sallittua vain, jos yhteisötilaaja on ennen käsittelyn aloittamista:

1) rajoittanut pääsyä 1 momentissa tarkoitettuihin tietoihin tai yrityssalaisuuksiin ja ryhtynyt muihin toimenpiteisiin tietojen asianmukaiseksi suojaamiseksi; ja

2) määritellyt, miten yrityssalaisuuksia saa siirtää, luovuttaa tai muutoin käsitellä sähköisessä viestintäverkossa ja minkälaisiin kohdeosoitteisiin 2 momentissa tarkoitettut henkilöt eivät ole oikeutettuja lähettämään yhteisötilaajan viestintäverkon kautta viestejä sekä laatinut tästä kirjallisen viestintäverkon tai viestintäpalvelun käyttäjälle annetun ohjeen.

Yhteisötilaaja saa käsitellä tunnistamistietoja automaattisen hakutoiminnon avulla. Automaattinen hakutoiminto voi perustua viestin kokoon tai viestien yhteenlaskettuun kokoon taikka viestien tyyppiin, määrään tai yhteystapaan taikka viestien kohdeosoitteisiin. Yhteisötilaaja voi hakea esille ja ottaa manuaalisesti käsiteltäväksi ne tunnistamistiedot, jotka ovat välttämättömiä yrityssalaisuuden paljastamisen ja siitä vastuussa olevien selvittämiseksi, jos:

1) automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama; tai

2) yrityssalaisuuden julkaisemisen tai sen luvattoman käytön taikka muutoin yleisesti havaittavissa olevien seikkojen perusteella on syntynyt perusteltu syy epäillä, että yrityssalaisuus on annettu luvattomasti ulkopuoliselle.

### 13 c §

#### *Yhteisötilaajan velvoitteet käsittelyoikeutta käytettäessä*

Yhteisötilaajan on ennen 13 a ja 13 b §:ssä tarkoitettua tunnistamistietojen käsittelyä nimettävä ne yhteisötilaajan viestintäverkon ja viestintäpalvelun ylläpidosta ja tietoturvas-

ta sekä yhteisötilaajan turvallisuudesta huolehtivat henkilöt, joiden tehtäviin tunnistamistietojen käsittely kuuluu tai määritellä mainitut tehtävät.

Yhteisötilaajan on laadittava 13 a ja 13 b §:ssä tarkoitettu manuaalisesta tunnistamistietojen käsittelystä siihen osallistuneiden henkilöiden allekirjoittama selvitys. Selvityksestä on käytävä ilmi käsittelyn peruste ja syy, minkä vuoksi tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty. Selvityksestä on lisäksi käytävä ilmi käsittelyn ajankohda, kesto ja käsittelijät sekä käsittelystä päättänyt henkilö. Selvitys on säilytettävä vähintään kaksi vuotta 13 a ja 13 b §:ssä tarkoitettua käsittelystä.

Edellä 2 momentissa tarkoitettu selvitys on annettava tiedoksi viestintäverkon tai viestintäpalvelun käyttäjälle heti, kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Selvitystä ei kuitenkaan tarvitse antaa niille käyttäjille, joiden tunnistamistietoja on käsiteltyssä käsitelty massamuotoisesti siten, että käyttäjien tunnistamistiedot eivät ole tulleet käsittelijän tietoon. Käyttäjällä on oikeus lakiin tai sopimukseen perustuvan salassapitovelvollisuuden estämättä luovuttaa selvitys ja sen yhteydessä saamansa tiedot etujaan tai oikeuksiaan koskevan asian käsittelyä varten. Yhteisötilaajan on annettava tietosuojavaltuutetulle:

1) ennen 13 a ja 13 b §:ssä tarkoitettujen tunnistamistietojen käsittelyn aloittamista selvitys, joka sisältää tiedot 13 a ja 13 b §:ssä tarkoitettujen yhteisötilaajan soveltamien menettelyjen perusteista ja käytännöistä sekä 13 c §:n 1 momentissa tarkoitetuista tehtävistä ja siitä, miten yhteisötilaaja tiedottaa näistä seikoista viestintäverkkojen ja viestintäpalvelujen käyttäjille; ja

2) vuosittain 13 a ja 13 b §:ssä tarkoitettua tunnistamistietojen manuaalisesta käsittelystä selvitys, josta tulee käydä ilmi, millä perusteella ja montako kertaa tunnistamistietoja on vuoden aikana käsitelty.

### 13 d §

#### *Työnantaja-asemassa olevan yhteisötilaajan ja työntekijöiden velvoitteet käsittelyoikeutta käytettäessä*

Jos yhteisötilaaja on työnantaja, on yhteisötilaajan sen lisäksi mitä 13 c:ssä § säädetään:

1) käsiteltävä yhteistoiminnasta yrityksissä annetun lain (334/2007) 4 luvussa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa (651/1988) ja työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa (449/2007) tarkoitetussa yhteistoimintamenettelyssä 13 a ja 13 b §:ssä tarkoitettujen yrityksessä sovellettavien menettelyjen perusteet ja käytännöt sekä 13 c §:n 1 momentissa tarkoitettut tehtävät ja tiedotettava käsitellyistä asioista tekemänsä päätökset työntekijöille tai heidän edustajilleen siten kuin yksityisyyden suojasta työelämässä annetun lain (759/2004) 21 §:ssä säädetään; ja

2) annettava työntekijöiden edustajille vuosittain 13 a ja 13 b §:ssä tarkoitettua tunnistamistietojen manuaalisesta käsittelystä selvitys, josta tulee käydä ilmi, millä perusteella ja montako kertaa tunnistamistietoja on vuoden aikana käsitelty.

Työntekijöiden edustajalla, jolle 1 momentin 2 kohdassa tarkoitettu selvitys on annettava, tarkoitetaan työ- tai virkaehtosopimuksen perusteella valittua luottamusmiestä tai, jos tällaista ei ole valittu, työsopimuslain (55/2001) 13 luvun 3 §:ssä tarkoitettua luottamusvaltuutettua. Jos jonkin henkilöstöryhmän työntekijät eivät ole valinneet luottamusmiestä tai luottamusvaltuutettua, tällaisen henkilöstöryhmän edustaja on yhteistoiminnasta yrityksissä annetun lain 8 §:ssä tai työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetun lain 3 §:ssä tarkoitettu yhteistoimintaedustaja taikka yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 6 §:n 2 momentissa tarkoitettu edustaja ja jos näitäkään ei ole valittu, selvitys on annettava kaikille tähän henkilöstöryhmää kuuluville työntekijöille.

Työntekijöiden edustajien ja 2 momentissa tarkoitettujen työntekijöiden on pidettävä salassa tietoonsa saamat yrityssalaisuuden loukkaukset ja epäilyt yrityssalaisuuden loukkaamisesta koko työsuhteen voimassaoloajan. Virkamiehen ja muun viranomaisen palveluksessa toimivan salassapitovelvollisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja muualla laissa säädetään. Mitä

edellä säädetään, ei estä tietojen luovuttamista valvontaviranomaiselle.

### 13 e §

#### *Yhteisötilaajan oikeus säilyttää tunnistamistietoja*

Mitä edellä 13 a ja 13 b §:ssä säädetään, ei oikeuta yhteisötilaajaa säilyttämään tunnistamistietoja rekisterissä kauempaa kuin lain mukaan muutoin on sallittua.

### 13 f §

#### *Yhteisötilaajan oikeus tietojen luovuttamiseen*

Sen estämättä, mitä 8 §:n 3 momentissa säädetään, yhteisötilaajalla on oikeus luovuttaa asianomistajana tekemänsä rikosilmoituksen tai tutkintapyynnön yhteydessä poliisille käsiteltäviksi 13 a ja 13 b §:n mukaisesti saamansa yhteisötilaajan viestintäverkon tai viestintäpalvelun käyttäjän viestejä koskevat tunnistamistiedot.

### 34 §

#### *Valvontaviranomaisten vaitiolovelvollisuus*

Viestintäviraston ja tietosuojavaltuutetun 33 §:n 3 momentin nojalla saamat tiedot luottamuksellisista viesteistä, tunnistamistiedoista ja paikkatiedoista sekä tietosuojavaltuutetun 13 c §:n 4 momentin nojalla saamat tiedot on pidettävä salassa.

Muilta osin valvontaviranomaisten tietojen salassapidosta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään.

### 42 §

#### *Rangaistussäännökset*

Rangaistus viestintäsalaisuuden loukkaamisesta ja törkeästä viestintäsalaisuuden loukkaamisesta säädetään rikoslain 38 luvun 3 ja 4 §:ssä sekä rangaistus tietomurrosta rikoslain 38 luvun 8 §:ssä. Rangaistus 5 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mu-

kaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla säädetä ankarampaa rangaistusta. Rangaistus 13 d §:n 3 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain (39/1889) 38 luvun 2 §:n 2 momentin mukaan, jollei teosta muualla kuin rikoslain 38 luvun 1 §:ssä säädetä ankarampaa rangaistusta.

Joka tahallaan

7) laiminlyö, mitä 25 §:ssä säädetään puhelinluetteloihin ja muihin tilaajaluetteloihin sisältyvien henkilötietojen käsittelystä, tilaajalle luettelon tarkoituksesta ja käytöstä ilmoittamisesta, tietojen poistamisesta ja korjaamisesta, kielto-oikeuksista tai oikeushenkilöiden oikeuksista,

8) harjoittaa suoramarkkinointia 7 luvussa säädetyn vastaisesti tai

9) laiminlyö, mitä 13 c §:ssä säädetään henkilöiden tai tehtävien nimeämisestä, selvityksen laatimisesta ja tiedoksi antamisesta ja tietosuojavaltuutetulle annettavista selvityksistä taikka mitä 13 d §:ssä säädetään asioiden käsittelemisestä yhteistoimintamenetelyssä ja työntekijöiden edustajalle annettavasta selvityksestä,

Tämä laki tulee voimaan päivänä kuuta 20

## 2.

**Laki****yksityisyyden suojasta työelämässä annetun lain muuttamisesta**

Eduskunnan päätöksen mukaisesti  
*muutetaan* yksityisyyden suojasta työelämässä 13 päivänä elokuuta 2004 annetun lain (759/2004) 2 §:n 3 momentti ja 21 §:n 1 momentti, sellaisena kuin se on laissa 457/2004 seuraavasti:

## 1 luku

**Yleiset säännökset**

## 2 §

*Soveltamisala*

—————  
 Työnantajan oikeudesta tilaajana saada maksuvelvollisuuden selvittämiseksi työntekijän käyttöön annettua liittymää koskevat tunnistetiedot ja oikeudesta käsitellä työntekijän sähköisen viestinnän tunnistetietoja luvattoman käytön tilanteissa ja yrityssalaisuuksien suojaamiseksi säädetään sähköisen viestinnän tietosuojalaissa (516/2004). Mitä mainitussa laissa säädetään paikkatietopalvelun käyttäjästä, sovelletaan työntekijään, jonka käyttöön työnantaja antaa paikkatietopalvelun. Henkilötietojen käsittelyyn sovelletaan henkilötietolakia (523/1999), jollei tässä laissa toisin säädetä.

—————

## 7 luku

**Erinäisiä säännöksiä**

## 21 §

*Yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä*

Työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely kuuluvat yhteistoiminnasta yrityksissä annetussa laissa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista.

—————

—————  
 Tämä laki tulee voimaan päivänä kuuta 20

—————

## 3.

**Laki****yhteistoiminnasta yrityksissä annetun lain 19 §:n muuttamisesta**

Eduskunnan päätöksen mukaisesti  
*muutetaan* yhteistoiminnasta yrityksissä 30 päivänä maaliskuuta 2007 annetun lain  
 (334/2007) 19 §:n 4 kohta seuraavasti:

## 19 §

*Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsitte-  
 ly*

sähköistä viestintää koskevien tietojen käsittely;  
 — — — — —

Yhteistoimintaneuvotteluissa tulee käsitellä:  
 — — — — —

\_\_\_\_\_

Tämä laki tulee voimaan päivänä kuuta 20

\_\_\_\_\_

4) sähköpostin ja tietoverkon käytön periaatteet sekä työntekijän sähköpostin ja muuta

## 4.

**Laki****yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 7 §:n muuttamisesta**

Eduskunnan päätöksen mukaisesti  
*muutetaan* yhteistoiminnasta valtion virastoissa ja laitoksissa 1 päivänä heinäkuuta 1988 annetun lain (651/1988) 7 §:n 11 a kohta, sellaisena kuin se on laissa 762/2004, seuraavasti:

## 7 §

*Yhteistoimintamenettelyn piiriin kuuluvat asiat*

telmät sekä sähköpostin ja tietoverkon käyttö sekä virkamiehen ja työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely;

Yhteistoimintamenettelyn piiriin kuuluvat:

11 a) henkilöstöön kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät mene-

Tämä laki tulee voimaan päivänä kuuta 20

Helsingissä päivänä kuuta 2007

**Tasavallan Presidentti**

**TARJA HALONEN**

Viestintäministeri